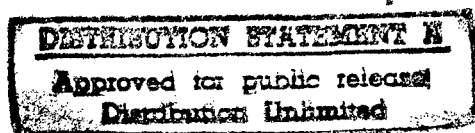


*The Defense Science Board
1997 Summer Study Task Force*

on

**DoD RESPONSES TO
TRANSNATIONAL THREATS**

**Volume I
Final Report**



DTIC QUALITY INSPECTED

19971230 109

October 1997

*Office of the Under Secretary of Defense
For Acquisition & Technology
Washington, D.C. 20301-3140*

This report is a product of the Defense Science Board (DSB). The DSB is a Federal Advisory Committee established to provide independent advice to the Secretary of Defense. Statements, opinions, conclusions and recommendations in this report do not necessarily represent the official position of the Department of Defense.

PLEASE CHECK THE APPROPRIATE BLOCK BELOW:

Please Process
PM
12/29/97

-AQ# *M98-03-0924*

☒ 1 copies are being forwarded. Indicate whether Statement A, B, C, D, E, F, or X applies.

☒ DISTRIBUTION STATEMENT A: *Per Lt Col Van Horn - 695-4157*
APPROVED FOR PUBLIC RELEASE: DISTRIBUTION IS UNLIMITED

☐ DISTRIBUTION STATEMENT B:
DISTRIBUTION AUTHORIZED TO U.S. GOVERNMENT AGENCIES ONLY; (Indicate Reason and Date). OTHER REQUESTS FOR THIS DOCUMENT SHALL BE REFERRED TO (Indicate Controlling DoD Office).

☐ DISTRIBUTION STATEMENT C:
DISTRIBUTION AUTHORIZED TO U.S. GOVERNMENT AGENCIES AND THEIR CONTRACTORS; (Indicate Reason and Date). OTHER REQUESTS FOR THIS DOCUMENT SHALL BE REFERRED TO (Indicate Controlling DoD Office).

☐ DISTRIBUTION STATEMENT D:
DISTRIBUTION AUTHORIZED TO DoD AND U.S. DoD CONTRACTORS ONLY; (Indicate Reason and Date). OTHER REQUESTS SHALL BE REFERRED TO (Indicate Controlling DoD Office).

☐ DISTRIBUTION STATEMENT E:
DISTRIBUTION AUTHORIZED TO DoD COMPONENTS ONLY; (Indicate Reason and Date). OTHER REQUESTS SHALL BE REFERRED TO (Indicate Controlling DoD Office).

☐ DISTRIBUTION STATEMENT F:
FURTHER DISSEMINATION ONLY AS DIRECTED BY (Indicate Controlling DoD Office and Date) or HIGHER DoD AUTHORITY.

☐ DISTRIBUTION STATEMENT X:
DISTRIBUTION AUTHORIZED TO U.S. GOVERNMENT AGENCIES AND PRIVATE INDIVIDUALS OR ENTERPRISES ELIGIBLE TO OBTAIN EXPORT-CONTROLLED TECHNICAL DATA IN ACCORDANCE WITH DoD DIRECTIVE 5230.25, WITHHOLDING OF UNCLASSIFIED TECHNICAL DATA FROM PUBLIC DISCLOSURE, 6 Nov 1984 (Indicate date of determination). CONTROLLING DoD OFFICE IS (Indicate Controlling DoD Office).

☐ This document was previously forwarded to DTIC on _____ (date) and the AD number is _____.

☐ In accordance with provisions of DoD instructions, the document requested is not supplied because:

☐ It will be published at a later date. (Enter approximate date, if known).

☐ Other. (Give Reason)

DoD Directive 5230.24, "Distribution Statements on Technical Documents," 18 Mar 87, contains seven distribution statements, as described briefly above. Technical Documents must be assigned distribution statements.

Defense Science Board 1997 Summer Study Task Force on DOD Responses to Transnational Threats Vol I, Oct 97

Print or Type Name

Authorized Signature/Date

Telephone Number



OFFICE OF THE SECRETARY OF DEFENSE

3140 DEFENSE PENTAGON
WASHINGTON, DC 20301-3140

DEFENSE SCIENCE
BOARD

9 Dec 97

Honorable Jacques S. Gansler
Under Secretary of Defense Acquisition and Technology
3010 Defense Pentagon
Washington, DC 20301-3010

Dear Mr. Secretary:

In response to joint tasking from the Under Secretary of Defense for Acquisition and Technology and the Chairman, Joint Chiefs of Staff, the 1997 DSB Summer Study Task Force addressed the Department's Responses to Transnational Threats. In the study, the Task Force concludes that the Department should treat transnational threats as a major Department of Defense mission.

Transnational actors have three advantages: 1) they can have ready access to weapons of mass destruction; 2) we cannot easily deter them because they have no homeland; and 3) they respect no boundaries, whether political, organizational, legal or moral. Further, warning may be short and attribution may be slow or ambiguous. Since the United States is now the dominant military force in the world, potential adversaries will be driven to asymmetric strategies to meet their objectives. As such, transnational threats represent an important national security problem.

Notably, the Department of Defense has the capacity to mitigate these threats with its extensive capabilities, training and experience. In the attached report, the Task Force suggests a multi-faceted strategy for the DoD to address this increasingly important class of threats. This strategy involves the development of an end-to-end systems concept, investment in critical technology areas, and the leveraging of similarities between civil protection and force protection. The Task Force concludes that the Department also needs to increase its emphasis on responding to this threat by more clearly assigning responsibilities and by providing mechanisms for measuring its readiness to respond.

We hope this Summer Study provides insights on how to mitigate transnational threats to the Nation. It stops short, however, of providing a plan. We strongly encourage the Department to take on the task of developing an implementation plan that identifies the appropriate allocation of resources and areas for emphasis.


Craig I. Fields
Chairman



OFFICE OF THE SECRETARY OF DEFENSE

3140 DEFENSE PENTAGON
WASHINGTON, DC 20301-3140

DEFENSE SCIENCE
BOARD

8 Dec 97

Memorandum for the Chairman, Defense Science Board

Subject: Final Report of the 1997 Defense Science Board Summer Study Task Force on DoD Responses to Transnational Threats

The final report of the 1997 Defense Science Board Summer Study Task Force on DoD Responses to Transnational Threats is attached. This report consists of three volumes: Volume I which presents the major findings and recommendations of the Task Force, Volume II which focuses on force protection and is written expressly for the Chairman, Joint Chiefs of Staff, and Volume III which includes eight supporting reports.

After focusing on this study topic for a period of six months, we concluded that threats posed by transnational forces are an important and under-appreciated element of DoD's core mission. We found a new and ominous trend -- a transnational threat with a proclivity towards much greater levels of violence. Transnational groups now have the means, through access to weapons of mass destruction and other instruments of terror and disruption, and the motives to cause great harm to our society. Since the United States remains the dominant military force in the world now, potential adversaries will be driven to asymmetric strategies in order to meet their objectives.

The Department of Defense has the capacity to mitigate these threats with its extensive capabilities, training and experience. We suggest that the DoD address this increasingly important class of threats through a response strategy that includes six elements:

1. Treat transnational threats as a major DoD mission
2. Use the existing national security structure and processes
3. Define an end-to-end operational concept and system-of-systems structure
4. Provide an interactive global information system on transnational threats
5. Address needs that have long been viewed as "too hard"
6. Leverage worldwide force protection and civil protection

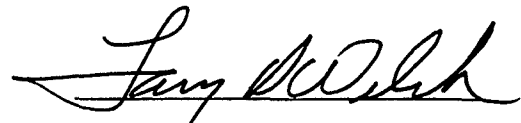
Together these principles will help the Department deal with transnational threats today and in the future. Notably, the task force holds that DoD can respond without a change to national roles and missions, and without change in its own organization. However, the DoD does need to increase its emphasis on this threat, clearly assign responsibilities and measure its readiness to respond. In addition, the

Department should focus more attention on strategies, architectures and plans that address the end-to-end set of capabilities needed.

We thank the Task Force members and the talented group of government advisors for their hard work and valuable insights. Their dedication reflects their belief in the importance of this challenge to the Department.



Robert Hermann, Chairman



Larry Welch, Vice Chairman

1997 DSB SUMMER STUDY

DoD Responses to Transnational Threats

"The dangers we face are unprecedented in their complexity. Ethnic conflict and outlaw states threaten regional stability. Terrorism, drugs, organized crime, and proliferation of weapons of mass destruction are global concerns that transcend national boundaries and undermine economic stability and political stability in many countries."

PRESIDENT WILLIAM J. CLINTON

"As the new millennium approaches, the United States faces a heightened prospect that regional aggressors, third-rate armies, terrorist cells, and even religious cults will wield disproportionate power by using – or even threatening to use – nuclear, biological, or chemical weapons against our troops in the field and our people at home."

SECRETARY OF DEFENSE, WILLIAM S. COHEN

TABLE OF CONTENTS

VOLUME I – FINAL REPORT

PREFACE	vii
EXECUTIVE SUMMARY	ix
CHAPTER 1: SETTING THE STAGE	1
Introduction.....	3
Role and Capabilities.....	5
CHAPTER 2: ORGANIZING A DoD RESPONSE	11
A Major DoD Mission	13
Existing Structures and Processes	23
Structuring the Operational and Technical Architectures	32
CHAPTER 3: TECHNICAL CHALLENGES	35
A Global Information Infrastructure.....	37
Addressing the “Too Hard” Problems	40
CHAPTER 4: SUMMARY OF RECOMMENDATIONS	57
ANNEX A: TERMS OF REFERENCE	A-1
ANNEX B: TASK FORCE ORGANIZATION AND MEMBERSHIP	B-1
ANNEX C: POLICY AND TECHNOLOGY RECOMMENDATIONS FOR ENHANCING DoD CAPABILITIES	C-1
ANNEX D: SUMMARY OF LAWS AND EXECUTIVE BRANCH GUIDANCE DOCUMENTS	D-1

VOLUME II – FORCE PROTECTION

PREFACE

EXECUTIVE SUMMARY

CHAPTER 1: INTRODUCTION

CHAPTER 2: PANEL ASSESSMENT

What is Force Protection?
Force Protection Environment
Force Protection Responsibilities
Current Force Protection Activities
Vulnerability Assessments – Lessons Learned
Next Steps

CHAPTER 3: ACTIONS REQUIRED

End-to-End Mission Orientation
Expand Vulnerability Assessments
Patch “Seams” Created by Diverse Responsibilities
Exploit Technology
Enhance Intelligence Operations

CHAPTER 4: FINAL THOUGHTS

ANNEX A. PANEL MEMBERSHIP

ANNEX B. BRIEFINGS AND REFERENCES

ANNEX C. J-34 FORCE PROTECTION PROGRAM

ANNEX D. SERVICE FORCE PROTECTION PROGRAMS

VOLUME III - SUPPORTING REPORTS*

THREATS AND SCENARIOS

SCIENCE AND TECHNOLOGY

DoD RESPONSE CAPABILITIES AND OPTIONS

Operational Intelligence Panel

Nuclear Panel

Biological Warfare / Chemical Warfare Panel

Physical, Launched, and Unconventional Means Panel

Information Warfare / Electronic Warfare Panel

Civil Integration and Response Panel

* Volumes 1 and 2 of this report represent the consensus view of this Task Force along with its analytical results and recommendations. Volume 3 of this report contains materials that were provided as inputs to the Task Force, but whose findings and recommendations may not represent the consensus view of this Task Force.

PREFACE

The Defense Science Board has examined new national security missions in the post Cold War period through a series of studies that began in 1995. In *Technology for 21st Century Military Superiority*, a task force examined Department of Defense (DoD) missions with an eye toward identifying where new investments would be appropriate to ensure military superiority. The 1996 Summer Study Task Force, in its report *Tactics and Technology for 21st Century Military Superiority*, examined ways to achieve substantial increases in the effectiveness of rapidly deployable forces and took a more comprehensive look at the missions identified in the 1995 report. This year's study continues the theme by looking at a new class of threats facing the United States in the 21st century.

Since the demise of the Soviet Union, the United States has been modernizing forces to address a wider range of missions and adversaries, to include some that are very different from those faced in the four decades following the end of World War II.

Perhaps less well appreciated, as highlighted in the 1995 study, these adversaries have also been modernizing their forces to discourage the United States and its coalition allies from influencing their foreign policy. They have lessons learned from Desert Storm. Their military modernization has included the purchase of large numbers of missiles and mines; some submarines with high speed torpedoes; the construction of underground facilities; and development of capabilities for weapons of mass destruction to include biological and chemical weapons. Coupled with their high tolerance for the loss of human life – both theirs and ours – their initiatives present a formidable challenge to long-term national security.

Even a small nation with a modest defense budget can afford such modernization. Last-generation weapons are still effective, particularly in large numbers. And last-generation weapons are much less costly than the more modern weapons. Coupling that with US requirements to be able to rapidly project force to unpredicted locations worldwide results in real problems to global security.

Further, potential adversaries employing inexpensive and much more readily available weapons of mass destruction can now use the global information infrastructure, along with the Global Positioning System and commercial imagery satellites, as their C3I system; and use the worldwide, robust commercial transportation infrastructure to project “force” anywhere, anytime. This can present a military capability as deadly as large conventional forces, and available – now – to very small adversaries, in terms of population, defense budget, and land area. In fact, it is available to adversaries with no claimed homeland – *the transnational threat*.

The transnational threat lies on a continuum ranging from violent domestic groups to belligerent nation states. It threatens the United States, US forces abroad, and allies. Such transnational threats, with political and economic agendas, and the willingness and ability to use

force and inflict mass casualties if necessary to achieve their goals, are better thought of as countries without land than as traditional terrorists.

For them, all war is global war. They can wage campaigns extending over years. Without fixed assets that we can hold at risk in their homeland, deterrence is difficult. Warning may be short. Attribution may be slow, ambiguous, or not achievable.

Transnational threats *do not* represent a new mission for DoD, but a different and difficult challenge to the traditional mission. In summary, transnational adversaries have three advantages: 1) they are willing to employ weapons of mass destruction; 2) they cannot easily be deterred; and 3) they respect no boundaries, whether political, organizational, legal, or moral.

This Summer Study suggests ways to help blunt this threat.

EXECUTIVE SUMMARY

With the change in the geopolitical structure of the Cold War, we are facing increased threats to the United States and its interests by organizations and individuals with motives and methods quite different than those posed to the nation during its confrontation with the Soviet Union. Among such threats are *transnational threats*: any transnational activity that threatens the national security of the United States – including international terrorism, narcotics trafficking, the proliferation of weapons of mass destruction and the delivery systems for such weapons, and organized crime – or any individual or group that engages in any such activity.

There is a new and ominous trend to these threats: a proclivity towards much greater levels of violence. Transnational groups have the means, through access to weapons of mass destruction and other instruments of terror and disruption, and the motives to cause great harm to our society. For example, the perpetrators of the World Trade Center bombing and the Tokyo Subway nerve gas attack were aiming for tens of thousands of fatalities.

While the task force clearly recognized the broader US government and coalition partner aspects of meeting the transnational threat, the scope of the subject was too large to include the full range of national and international issues in this single effort. Hence, the task force generally limited its focus to DoD's capabilities and responsibilities – a large enough set of issues.

Threats posed by transnational forces can interfere with DoD's ability to perform its mission, to protect its forces, and to carry out its responsibilities to protect the civilian population. Defense against transnational threats is part of DoD's core business. The Department has the capacity to contribute to the mitigation of these threats with its extensive capabilities, training, and experience. And the Department of Defense has been called out in law to participate in the response to transnational threats.

This Defense Science Board study principally addresses DoD capabilities, options, and responses to transnational threats. It recommends a long-term strategy for DoD's response that leverages the Department's resources and strengths. That strategy is provided in this report. The task force recommends that DoD take on the challenge of developing plans and allocating resources to implement the strategy outlined in the chapters to follow.

The task force addressed the DoD response strategy using six elements:

- 1. Treat transnational threats as a major DoD mission**
- 2. Use the existing national security structure and processes**
- 3. Define an end-to-end operational concept and system-of-systems structure**
- 4. Provide an interactive global information system on transnational threats**
- 5. Address needs that have long been viewed as "too hard"**
- 6. Leverage worldwide force protection and civil protection**

Together, these principles form the structure to help position DoD to meet its responsibilities in dealing with transnational threats of today and the future. Notably, the task force holds that DoD can respond without a change to national roles and missions and without change in its own organization. The discussion which follows expands on these six elements.

Organizing a DoD Response

A Major DoD Mission

Examples of the transnational threat are familiar to us all. Events such as the 1983 attack on the US Marine Corps barracks in Beirut, Lebanon, and the 1996 bombing of Khobar Towers in Saudi Arabia are recent cases of significant consequence. The task force believes that the transnational threat will escalate in the future and be increasingly characterized by planned campaigns designed to inflict maximum damage and casualties.

US presence, policies, and leadership must remain a major stabilizing force in the world, and as such, overseas US military operations will continue to be the norm. The Department of Defense must recognize and deal with an escalating and more dangerous threat environment and its impact on missions overseas as well as within the United States. While the task force focused on DoD responsibilities, the national leadership – to include the President – will need to provide vigorous leadership in preparing for this set of threats.

The increased DoD attention needs to include transnational threats in departmental guidance and strategy, in the planning and budgeting processes, and in training and exercises. This is not a new mission for DoD, but the capabilities and motives of these transnational adversaries raise the challenge to a far higher level.

Existing Structures and Processes

The transnational threat challenge requires a “three-tiered” response: global, regional, and force level. This response should capitalize on the parallelism between domestic preparedness, global force protection, force projection, and a major theater war. There is strong synergy between the demands of each. A robust force protection capability is critical to meet US security needs and maintain the nation’s ability to project its forces abroad. The requirements, procedures, and technology for protecting military facilities against attacks by transnational forces have much in common with protecting civilian facilities in metropolitan areas. Thus, the United States can leverage DoD capabilities and expertise for both force protection and to contribute more effectively to civil protection.

Force protection is a major responsibility for the Department of Defense, for its forces at home and abroad. The Department has taken steps to improve its force protection programs as the new threat emerged. DoD deserves high marks for these efforts to date, but there is still much

to accomplish. An enhanced force protection program demands an end-to-end mission orientation, expanded vulnerability assessments, patching the "seams" created by diverse responsibilities, focusing intelligence programs and capabilities, and exploiting promising technologies.

Civilian protection begins with the local and state first responder community – law enforcement, fire and rescue, medical, and emergency management personnel. Both the Department of Defense and civilian communities can benefit from improving the integration between the local, state, and federal agencies. Improvements in communication, training, information sharing, operations, and resource transfers would help to streamline emergency response operations and interfaces across all levels of responders. This will involve developing a plan to expand the scope of the Nunn-Lugar-Domenici program and institutionalizing it within the Department.

Also, utilizing state-level assets such as the National Guard more effectively can serve to strengthen the linkages between civil protection and force protection with benefit to all participants. Specifically, the Guard should establish a national consequence management capability to support state and local agency responses to domestic incidents, particularly those involving chemical or biological agents, and to support sustainment training and exercises with first responders.

DoD can and should respond to the escalating transnational threat challenge using the existing national security structure and processes. But within this structure, the Secretary of Defense should clarify responsibilities throughout the organization for policy coordination, operations, and research and development. Today, multiple offices within the Department are involved in each mission area, with no one effectively positioned to ensure the most effective DoD posture against the threat.

Structuring the Operational and Technical Architectures

The elements necessary to respond to the transnational threat exist within the Department of Defense, as does the expertise. But DoD needs a more comprehensive plan – an end-to-end operational architecture – to refocus varied and diverse elements throughout the Department and to prepare a cohesive, strategic response to the transnational threat.

This planning activity is to define the interfaces between crisis management (pre-event) and consequence management (post-event) to ensure there is no gap. It must identify technology needs and requirements and must identify priorities for research and development, acquisition, exercises, training, and "red teaming" to provide a sound basis for an investment strategy, while effectively leveraging available resources within DoD.

Technical Challenges

An important part of improving DoD's capability to respond to the transnational threat includes drawing on and incorporating technological advances into the Department's response arsenal. In the case of this unique threat, this may mean taking on problems that have long been viewed as too difficult – either bureaucratically or technically.

A Global Information Infrastructure

The United States must get smarter about the transnational threat. The task force sees a need for an interactive, two-way global information system that would expand the available sources of information. This information system would support gathering more data from the bottom up, exploit international information sources, and facilitate the sharing and analysis of information collected by different organizations. This would mean global distributed data bases, held at numerous security levels, and accessible by a global information sharing community focused on deterring and dealing with the wide spectrum of potential transnational threats.

The United States can exploit the information technology available today to develop a global information system that would permit real-time, collaborative analysis and correlation of information. Such a system – which the task force termed the Secure, Transnational Threat Information Infrastructure – can be developed based on the technology and infrastructure available today from the World Wide Web, and into which many agencies and organizations are already connected.

Addressing the “Too Hard” Problems

There are a number of challenges that have historically been regarded as “too hard” to solve: the nuclear terrorism challenge, defense against the biological and chemical warfare threat, and defense against the information warfare threat. This task force believes that these challenges should be addressed and that doing so will make a substantive difference in the nation's ability to respond to these distinctly different and serious threats.

In addressing these challenges, the United States must avoid being trapped into inaction because the problems are difficult. Measuring the effectiveness of actions against only the most stressful threat or embracing only the “perfect” solution can stand in the way of important progress. An incremental approach for improving America's capabilities to deal with the nuclear, chemical, and biological transnational threats is prudent and is ardently needed to reduce the enormous potential consequences from such attacks.

The Nuclear Challenge. If the required fissile material is available, it is not difficult to design and build a primitive nuclear explosive device. Knowledge about the design and use of nuclear weapons is available in the public domain to an ever-widening clientele. Insuring the security of nuclear weapons and materials in Russia and the states of the Former Soviet Union is

crucial and thus the task force endorses the aggressive continuation of the Nunn-Lugar nuclear safeguard initiatives begun several years ago.

The task force believes that with a continued, comprehensive long-term program, capabilities can be developed – jointly with the Department of Energy – to deal effectively with this threat over a wide range of possible scenarios. Throughout the process of building and transporting a nuclear device, there are signatures which can be exploited by improved intelligence, law enforcement operations, and enhanced detection capabilities. An improved posture to defend against the nuclear transnational threat includes many elements: information and intelligence, security, detection, disablement, mitigation, and attribution. A comprehensive program, developed within the overall architecture for responding to transnational threats, should integrate each of these elements.

The Chemical and Biological Warfare Threat. Chemical and biological warfare agents share characteristics that make them an especially grave threat. They are relatively easy to obtain, can be developed and produced with modest facilities and equipment, can be lethal even in small quantities, and can be delivered by a variety of means. But they also have substantial differences which must be taken into account when devising strategies and postures to deal with the threat. For example, biological agents can be far more toxic while the lethal effects of chemical agents typically occur more rapidly than biological warfare agents. A focus on incremental steps to mitigate this threat and raise the price to potential attackers will require a sustainable and productive defense effort for the long term. While there are many promising steps to take, there is no silver bullet.

The task force endorses the Secretary of Defense's intent to add \$1 billion to the chemical and biological defense program as recommended in the Quadrennial Defense Review. Areas where immediate action might be taken with such an increase include: augmenting the Technical Escort Unit to expand readiness, enhancing medical teams in the Army, conducting more exercises and instituting red-team testing for chemical and biological warfare defense, developing operational decontamination standards, supporting the Technical Support Working Group emphasis on chemical and biological warfare defense and force protection, engaging the biotechnology industry via a direct Presidential appeal, and establishing a threat reduction program with the Russian biological warfare community – in effect extending Nunn-Lugar beyond nuclear materials and weapons into biological materials, processes and weapons. In addition, the effort on the biological warfare threat in the intelligence community should be greatly increased.

Information Warfare Threat. The transnational information warfare threat also poses significant technical challenges. Tools and techniques for penetrating networks illicitly are rapidly becoming more sophisticated and varied, the associated software tools are available, and there is a community eager to share and exploit these tools. The intended effects of an information warfare attack probably will not be subtle, particularly in the context of a carefully orchestrated information warfare campaign. Such a campaign will become increasingly likely. Probable scenarios could couple an attack using chemical or biological weapons with information disruption of the warning and response processes.

DoD's current network security posture is inadequate and the Department's unclassified networks have been compromised on a number of occasions over the last decade. The Department must build the capability to improve its information protection abilities faster than the threat can create new methods for attack. This requires that processes for continuous improvement and organizational learning – training, exercises, and red teaming – be an integral part of any DoD information assurance program. Because DoD cannot function in isolation, these concerns must be addressed in a way that enables the Department to cooperate and share information with other government agencies, the private sector, and allied governments.

In summary, the task force concludes that transnational threats can be as serious as those of a major military conflict. Combating transnational threats is part of the Department of Defense's core business, and DoD can meet these challenges using existing policies and organizations. An effective national response to the transnational threat and implementation of the six-element strategy requires a dedicated effort on the part of the national leadership to include senior leadership in the Department of Defense. Such an integrated, focused, and committed response will prepare the Department and the Nation to blunt the transnational threat.

CHAPTER 1.

Setting the Stage

"This isn't a new problem, it is simply an old problem getting worse. Those out to do us harm are no longer just political zealots with a few sticks of dynamite. These are determined operatives, with access to very sophisticated information and technology. Unable to confront or compete with the United States militarily, they try to achieve their policy objectives by exploiting small groups to do the dirty work for them."

CHAIRMAN, JOINT CHIEFS OF STAFF,
GEN JOHN M. SHALIKASHVILI, USA

CHAPTER 1. SETTING THE STAGE

Introduction

As the geopolitical structure of the Cold War collapsed, the environment fostered the rise of radically new threats to the United States and its interests by organizations and individuals with motives and methods quite different than those posed to the nation during its confrontation with the Soviet Union. These threats, referred to throughout this report as *transnational threats*, comprise any transnational activity that threatens the national security of the United States – including international terrorism, narcotics trafficking, the proliferation of weapons of mass destruction and the delivery systems for such weapons, and organized crime – or any individual or group that engages in any such activity.¹

The motives and methods of the transnational threat are different from those of traditional nation states.² The technology of today, and that which is emerging, allows a small number of people to threaten others with consequences heretofore achievable only by nation states. The United States' homeland, allies, and interests are vulnerable. In the judgment of this task force, the likelihood and consequences of attacks from transnational threats can be as serious, if not more serious, than those of a major military conflict. Defense against transnational threats is part of DoD's core business, and must command the attention of the nation's leaders.

A component of what makes these threats different is that they are difficult to deter, detect, and control. The difficulty of attribution that arises with transnational threats allows attacks against the United States and its allies that nation states would not risk directly for fear of retaliation. As such, national boundaries are not effective barriers, and are used to the adversary's advantage. This situation results in the denial of an entire arsenal of traditional and well-developed political, diplomatic, and military strategies for addressing threats to our nation.

An effective response to these threats requires the interaction of the federal, state, and local law enforcement and emergency response agencies; the broader national security community; and the international community – agencies and parts of society that have had little history of integrated planning, strategy, or action. The collective efforts of these organizations will play an important role in increasing the nation's security against transnational threats. This study includes some recommendations on how to formulate this collective response.

¹ This definition of transnational threats is taken from Public Law 104-293, 1996 HR 3259, Section 804.

² The Threats and Scenarios Chapter in Volume III contains an expanded discussion of the future threat.

At the request of the Chairman, Joint Chiefs of Staff and the Under Secretary of Defense for Acquisition and Technology, this task force assessed the DoD posture in response to transnational threats and recommended actions to improve this posture.³ Specifically, the task force was asked to:

- Review the legislation, executive orders, prior studies, and current activities of the government;
- Identify the variety of threats which should be addressed by the Department;
- Assess the nation's vulnerability to these threats;
- Examine the DoD capabilities for playing its proper role in response;
- Identify available and potential technologies that may be applicable for enhancing the protection of US Armed Forces; and
- Recommend actions by the Department to position itself properly for this set of problems.

This study addresses DoD capabilities, options, and responses to transnational threats. It recommends a long-term strategy for DoD's response that leverages the Department's resources and strengths. This task force has focused its recommendations on issues concerning the Department of Defense and has not attempted to address Government-wide issues. Also beyond the scope of this effort is a detailed analysis of information operations, the topic of a 1996 Defense Science Board study *Information Warfare-Defense*, the recommendations of which are supported by this task force.

The expansive scope of this year's study called for an unusually large task force, with expertise drawn from a wide range of disciplines. Participants included experts in intelligence, weapons of mass destruction, information warfare, policy, science and technology, and force protection and included a sizable group of government advisors drawn from across the national security community. In addition, the task force had representatives from the civilian first responder, law enforcement, and emergency management communities to provide their unique perspective on this important topic, which bridges the military and civilian communities.⁴

In this study, the task force set out to develop a strategy for the Department of Defense to respond to the transnational threat and to raise the level of emphasis devoted to this important national problem. That strategy is provided in this report. The task force recommends that DoD take on the challenge of developing a responsive, end-to-end operational and technical architecture and associated plans to implement the strategy outlined in the chapters to follow.

³ Annex A contains the complete Terms of Reference for the Defense Science Board 1997 Summer Study.

⁴ A list of task force members is in Annex B.

Role and Capabilities

So, why should the Department of Defense be engaged?

- 1) It is part of DoD's core business. The nature and seriousness of this threat make countering transnational adversaries itself a DoD mission. Further, threats posed by transnational adversaries can interfere with DoD's ability to perform other missions, to protect its forces, and to carry out its responsibilities to protect the civilian population.
- 2) DoD has the capacity to contribute extensively to the mitigation of these threats, whether the response involves circumstances where DoD is in the lead, or where the Department is in a supporting role.
- 3) DoD has unique capabilities including: widely distributed assets such as intelligence, equipment, and standing forces – active and reserve – and assets such as the National Guard and state militia; experience with organizing, equipping, training and operating forces in high stress, life-threatening environments that can be brought to bear in both domestic and international situations; and extensive capability-building potential on a global level.
- 4) DoD has unique expertise in weapons of mass destruction.

The Department of Defense has also been called out in law to be a participant in the response to transnational threats.⁵ The Nunn-Lugar-Domenici law, PL104-293, identifies the Secretary of Defense as a member of a national-level committee on transnational threats and lays out other specific responsibilities for the Department of Defense. The task force strongly endorses the Nunn-Lugar-Domenici initiative and recommends that DoD retain stewardship of this important program in the years ahead.

Today's Capabilities

DoD has many resources that can support both crisis management (pre-event) and consequence management (post-event) in responding to the transnational threat. For DoD, crisis management encompasses tasks necessary to interdict, isolate, move, or destroy a weapon of mass destruction and collect evidence for legal prosecution. Consequence management includes those DoD assets that can assist with protecting emergency responders, identification of agents, decontamination of casualties, medical triage and stabilization, and perception management.

During the past few years, the Department has undertaken many activities to improve these capabilities. A number of these initiatives enhance DoD's ability to respond to and mitigate incidents involving weapons of mass destruction, with particular emphasis on chemical and

⁵ A summary of relevant legislation and executive branch guidance documents is included in Annex D.

biological agents. Others involve changes in the Department's organizational responsibilities that focus attention and action on the transnational threat. DoD participation in interagency activities and interagency forums is another area with ongoing initiatives. Some examples are highlighted below.

In 1996, the US Marine Corps Chemical Biological Incident Response Force (CBIRF) was created. This group of over 300 Marines is based on the East Coast and has been used on several occasions to respond to incidents, or to stand ready at events such as the Atlanta Olympics and the Denver G-8 conference. The Army has significantly increased the operations of its Technical Escort Units – the Army's chemical and biological response units – which support hazardous materials spills or chemical/biological incidents of one kind or another.

An advanced concept technology demonstration, known as 911-BIO, involves the Army and Marines, and is examining improved capabilities in detecting and responding to biological agents. The demonstration is a two-part effort to help accelerate the fielding of bio detectors and related technologies. The program also seeks to provide a venue to allow the Marine Corps Chemical Biological Incident Response Force and the Army's Technical Escort Unit to develop and refine operational procedures.

The Air Base/Port Detector Biological Defense Program, another advanced concept technology demonstration, seeks to provide and demonstrate important bio detection capability for force protection. In this demonstration, an air base in South Korea and a base in Southwest Asia will be surrounded by a ring of integrated monitors that have the capability of providing sufficient warning of an approaching biological agent to allow base personnel to take shelter or don protective equipment. Both of these technology demonstrations, and others like them, will be important in accelerating the fielding of detectors, protective equipment, and decontamination capability to support both protection of US military forces and the domestic first responder community.

Other efforts include DARPA's \$50-60 million per year research and development program on biological warfare defense. The Defense Department has established a cooperative agreement with the Department of Energy covering research and development activities for chemical and biological warfare defense. And the Secretary of Defense supports a \$1 billion increase in the budget for chemical and biological warfare defense, a recommendation from the Quadrennial Defense Review.

The Department has also made some explicit assignments of responsibility for addressing transnational threats. The regional Commanders-in-Chief are now involved with the Joint Special Operations Task Force, which is focused on crisis management, and the Response Task Force, which focuses on consequence management, both of which were deployed for the first time at the Denver G-8. The J-34, a new division within the Joint Staff, was created to focus on the mission of combating terrorism. Among their activities are assessments of the vulnerability of military installations to transnational threats. These assessments, conducted on behalf of the Joint Staff

by the Defense Special Weapons Agency, involve physically visiting facilities and evaluating all aspects of vulnerability. Written assessments with recommendations for mitigating risk and reducing vulnerabilities are provided to local commanders.

Interagency activities include an active and growing role for the Technical Support Working Group (TSWG), with representation that cuts across many agencies and is drawn from throughout the Department of Defense. This group sponsors near-term research, development, and rapid prototyping of technologies to counter transnational threats.

The Nunn-Lugar-Domenici legislation established a series of initiatives to involve DoD and other federal agencies in responding to transnational threats, with focus on an actual crisis and in dealing with the consequence of a crisis were one to occur. Details of this legislation are discussed further in Chapter 2.

Despite the activity represented by the many initiatives discussed above, the task force is concerned about the *erosion* of the structure underlying many of DoD's critical capabilities to deter and defend against transnational threats. For example, nuclear capabilities are a less valued specialty in the military services, but are an important aspect of dealing with this problem. While the operations of the Technical Escort Unit have substantially increased, staffing of the unit has not. This unit has been deployed over 200 days a year, further personnel reductions are planned, and the increasing mix of civilians in the unit detracts from its ability to quickly respond in a crisis.

Chemical and biological capabilities in the Department are stretched thin. In the area of chemical warfare, the pressure on existing capability is significant. The Marine Chemical Biological Incident Response Force now employs about 60 percent of the nuclear, biological, and chemical specialists of the Corps. In the active units of the Army, research and development and medical reductions are ongoing as part of the overall downsizing in DoD, diminishing capabilities available to support requirements of the regional Commanders-in-Chief. In the Defense Intelligence Agency, an increase of 50 people to focus on the counterterrorism problem included only one specialist dedicated to the chemical and biological area. The closing within the next decade of eight chemical storage sites will reduce response capabilities to chemical incidents, including accidents, and will have a concomitant impact on civilian protection capabilities. These sites have emergency response plans that have been created with involvement of the local community, and there is a large body of knowledge resident there. It will be critical to begin transferring such knowledge to other DoD installations and local organizations, lest it be lost.

The task force believes that DoD's biological capability is especially vulnerable. This small base of expertise cannot withstand a "fair share" of the cuts. Only six professionals in the United States Army Medical Research Institute of Infectious Diseases (USAMRIID) support the operational medical needs of the regional Commanders-in-Chief. In this environment, recruiting and retaining world class people is very difficult.

In summary, DoD has many unique capabilities to help thwart or reduce the consequences of attacks from transnational forces. There are many activities ongoing that are relevant to dealing with this threat, but the Department is on a steep learning curve. The current level of effort falls short of what is needed and some critical capabilities are eroding. The Department's role will vary, with DoD most often playing a supporting role on US soil, but in charge of force protection abroad. In any scenario, DoD will logically be a major player. As such, the Department should be committed for the long term.

Tomorrow's Challenge: Six Organizing Principles

The US response to transnational threats involves both an offensive and defensive component. The nation's goal is to use whatever tools it can to shape the environment, to deter transnational threats, to detect and interdict activities, to protect its forces and civilian population, and if an incident does occur, to mitigate its consequences. Different types of threat require a different response, drawing on the nation's wide range of capabilities, including those of DoD.

This DSB task force sees a need for strengthening DoD's response capabilities and has identified six elements of a DoD response strategy, each of which will be discussed in detail in subsequent chapters. They are listed here:

1. Treat transnational threats as a major DoD mission
2. Use the existing national security structure and processes
3. Define an end-to-end operational concept and system-of-systems structure
4. Provide an interactive global information system on transnational threats
5. Address needs that have long been viewed as "too hard"
6. Leverage worldwide force protection and civil protection

Together, these principles form the structure for effectively positioning DoD against the transnational threats of the future. Notably, the task force holds that DoD can respond without change to national roles and missions and without change in its own organization.

The following chapters discuss the six elements of a DoD response strategy. Chapter 2 examines the first three elements which focus on organizing for a DoD response: prioritizing the threat, assigning roles and responsibilities, and developing a concept of operations and architecture to guide the Department's actions in the future. This chapter also examines the parallelism between force protection and civil protection. In Chapter 3, key technical challenges are discussed: developing a global information infrastructure and responding to the difficult threat posed by weapons of mass destruction and information warfare. The final chapter summarizes the task force recommendations as actions for the Department's leadership. These

are the steps that DoD needs to take in order to have an effective response capability to the transnational threats of today and the future.⁶

⁶ Volumes II and III offer more detailed discussions of the topics presented in this volume.

CHAPTER 2.

Organizing a DoD Response

"He related to us that during World War II, the Americans had dropped the atomic bombs on the cities of Hiroshima and Nagasaki, killing 250,000 civilians, and he said that the Americans would realize if they suffered those types of casualties that they were at war."

SECRET SERVICE AGENT BRIAN PARR RECOUNTING RAMZI AHMED YOUSEF'S ADMISSION TO THE WORLD TRADE CENTER BOMBING

CHAPTER 2. ORGANIZING A DoD RESPONSE

A Major DoD Mission

The Threat

Examples of transnational attacks over the past decade are familiar to all, as illustrated below in Figure 1. Looking carefully at these events and their motivations, three lessons emerge. *First, some transnational attacks reflect attempts by transnational adversaries to influence American foreign policy.* The 1983 attack on the US Marine Corps barracks in Beirut, Lebanon; the attack on US forces in Somalia in 1993; and the 1996 bombing of Khobar Towers in Saudi Arabia are recent examples.

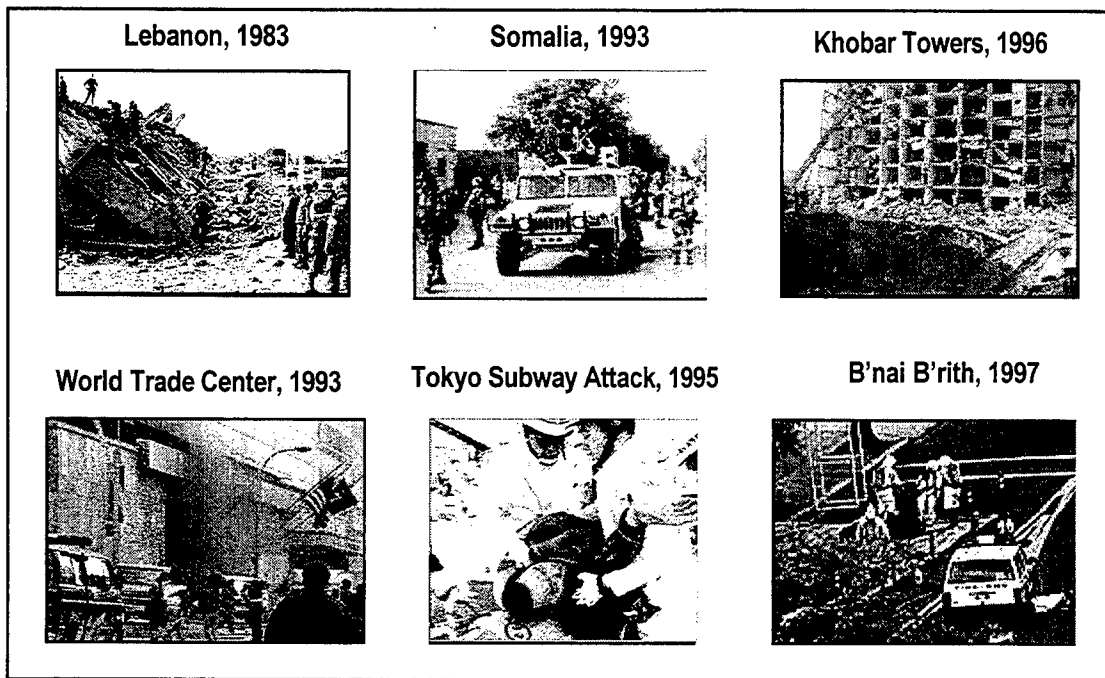


Figure 1. Examples of the Transnational Threat

Second, other incidents illustrate the many capabilities in the hands of transnational adversaries: explosives, chemical, and biological agents. In 1995, the world witnessed the release of the chemical agent sarin in the Tokyo subway. While the chemical release killed a dozen people, well over 5,000 were injured and the release had the potential for far more devastating loss of life. In fact, the plan was for tens of thousands of deaths. And closer to home, incidents like the 1993 World Trade Center bombing, the 1996 bombing of the Murrah Building in Oklahoma City, and the 1997 incident at the B'nai B'rith building in downtown Washington DC, which involved a container purported to hold anthrax, show the breadth of weaponry available.

Further, they demonstrate that the United States is no longer a sanctuary and is vulnerable on its own soil as well.

A third lesson is that *transnational adversaries, in contrast to traditional terrorists, are motivated to inflict massive destruction and casualties*. In the past, analysts believed one of the key "tenets of terrorism" was that terrorists calculated thresholds of pain and tolerance, so that their cause was not irrevocably compromised by their actions. While US government officials worried about terrorists "graduating" to the use of weapons of mass destruction (almost exclusively nuclear), they believed – based on reports from terrorists themselves – that most terrorist groups thought mass casualties were counterproductive. Mass casualties were believed to delegitimize the terrorists' cause, generate strong governmental responses, and erode terrorist group cohesion. In essence, terrorists were ascribed a certain logic and morality beyond which they would not tread. The world has changed and this mentality is no longer the case.

The transnational threat is more acute today for a variety of other reasons. An important factor is *the global proliferation of military-related technology and knowledge*. Knowledge about production and use of weapons of mass destruction – nuclear, chemical, biological, and radiological – as well as targeting information, is available in the public domain to an ever-widening clientele. In addition, the rapid proliferation across the world of industries and technologies with both civilian and military application fuels the transnational threat – making the future threat different and more dangerous than the old.

Moreover, modern commercial information technologies facilitate access to military-related technology and facilitate communications among transnational adversaries regardless of their location. Transnational groups are increasingly linked in new and more cooperative ways that threaten the stability of governments, the financial and information infrastructure, and international trade and peace agreements. Increasing cooperation among crime, narcotics, and terrorist groups has provided transnational adversaries with new, more creative ways to raise money and with a marketplace to shop for weapons and high technology equipment.

An increasing number of world actors devoted to political, economic, and ethnic disruption also contributes to a growing threat environment. Transnational groups include classic terrorists, ethnic groups, religious extremists, anti-government militia, narcotic traffickers, and global criminals. Attacks without attribution are on the rise, and hate groups and religious extremists are growing in numbers. US policies in the Middle East have become the basis for violent retaliation from many groups. The goals of many of these groups are guided by a different moral compass; maximum damage and destruction is morally justified by their "higher" purpose.

In addition, *the United States is more vulnerable to transnational threats today* than in the past, and this is likely to grow. This vulnerability has increased as critical infrastructure is consolidated and becomes more interdependent. Further, the US government and its security structure depend more on civilian and commercial systems in response to the rising costs of buying and maintaining systems designed specifically for the military. The revolution in

information sciences plays a role, increasing dependency on information technology and vulnerability to cyber threats.

As part of its global super power position, the United States is called upon frequently to respond to international causes and deploy forces around the world. America's position in the world invites attack simply because of its presence. Historical data show a strong correlation between US involvement in international situations and an increase in terrorist attacks against the United States. In addition, the military asymmetry that denies nation states the ability to engage in overt attacks against the United States drives the use of transnational actors.

Another component of US vulnerability is that Americans tend to view transnational threats singularly. That is, terrorist incidents, even those as attention-grabbing as the New York City Trade Center bombing, tend to look like individual events that do not evidence a campaign against US policies or interests. Deeper investigation shows that a number of transnational adversaries have planned campaigns of unconventional warfare. And the United States will remain a significant target for such groups in the future.

Finally, *a number of "global stresses" in the twenty first century will impact the range and scope of transnational threats.* Population growth increases demand on infrastructures, water, energy, and select territories. Global economic growth will continue to spur economic disparity between societies because the growth is predicted to be uneven on a regional, national, ethnic, and social status basis. Occasional "failed states" will fuel domestic disorder, mass cross-border migration, and mass humanitarian needs. Some nations will face diminishing authority and influence as a result of global economic, political, and military shifts.

The transnational threat is real, as has been revealed through many international incidents. The United States has been warned. Three examples serve to illustrate the nature and severity of this threat. Each case – the Libyan retaliation campaign, the World Trade Center bombing, and the Aum Shinrikyo subway sarin release – helps to explain the many facets of the threat and the changing nature of motivations of transnational adversaries.

Libya Retaliation Campaign. When evidence pointed to Libya as the culprit behind the LaBelle Disco bombing in Berlin, which killed two US soldiers and injured many, the United States retaliated with an air strike in April 1986 against specific Libyan targets in Tripoli. The popular belief for years was that this US attack suppressed Libyan activity in support of terrorism. However, an examination of events in subsequent years paints a different picture. Instead, Libya continued, through transnational actors, to wage a revenge campaign over a number of years as summarized in Figure 2.

Three days after the US attack, Libyan retaliation began. An American hostage in Lebanon was sold to Libya and executed. In September 1987, Abu Nidal, working for Libya, hi-jacked Pan Am 73 causing the death of several Americans. The following April, the Japanese Red Army, under contract to Nidal, bombed the USO in Naples, killing a US soldier. While attempting to

coordinate activities, a member of that group was arrested in New Jersey with pipe bombs targeted for New York City. The December 1988 bombing of Pan Am 103 – killing 270 people, 200 of whom were Americans – was a Libyan-sponsored act. A year later, in September 1989, a UTA French airliner was destroyed over Chad by the same group. During this period, this group was also responsible for various assassinations of dissident Libyans in the United States. It also recruited a Chicago street gang to attack US airliners with shoulder-fired weapons – a move that was interdicted.

Qadhafi sponsored this series of attacks, using surrogates for plausible denial. While these acts involved the backing of a nation state, Libya, it did not involve traditional military force. It illustrates the ability and willingness of transnational adversaries to wage a continued campaign against the United States, one that the United States, in this case, was only partially successful in countering.

Retaliation while avoiding consequences

- ♦ Apr 86 — Bombed the LaBelle Disco in Berlin – reaction to President Reagan's charges against Qadhafi – US retaliated against targets in Libya
- ♦ Libyan retaliation using surrogates started three days later
 - US hostage in Lebanon sold to Libya and executed
 - Sept 87 — Pan Am 73 hi-jacked by Abu Nidal working for Libya – several Americans killed
 - Apr 88 — Japanese Red Army working for Abu Nidal
 - USO bomb in Naples killed a US sailor
 - Member arrested in New Jersey with pipe bombs targeted for New York City
 - Dec 88 — Pan Am 103 – kills 270 (200 Americans)
 - Sept 89 — UTA French airliner destroyed over Chad
 - Same two that blew up Pan Am 103
- ♦ Recruited Chicago street gang to attack US airliners with shoulder-fired weapons
 - Interdicted

Figure 2. Libya Retaliation Campaign

World Trade Center Bombing. The motive for the religious extremists involved was to punish the United States for its policies in the Middle East. Their goal was to create maximum casualties and damage.

In May 1990, a small band of religious extremists headed by Ramzi Yousef assassinated Rabbi Meir Kahane. At the time, the rabbi's death was treated as a homicide, unrelated to national security. It was only later that this assassination was discovered to be part of a larger revenge campaign against US foreign policy that included the World Trade Center bombing in February 1993. Six people were killed and five thousand were injured, but the terrorists' plans were to kill

250,000 through the collapse of the towers, as Figure 3 illustrates.⁷ Fortunately the building structure was far more robust than they calculated. They also considered augmenting the explosion with radiological materials or chemical agents, which would have pushed the number of casualties far higher.



Figure 3. World Trade Center

In addition to the World Trade Center event, this transnational group had planned a massive infrastructure attack on New York City on the Fourth of July that would have included attacks on the George Washington Bridge, Lincoln and Holland Tunnels, the United Nations Headquarters, and the Federal Building in New York. These acts were interdicted through intelligence and surveillance.

The architect of this campaign, Ramzi Yousef, evaded capture for two years, but is now in the hands of US officials and standing trial. His plans were not limited to attacks on New York City, but involved a series of follow-on events to include an attack on thirteen international flights using explosives smuggled aboard. This particular activity was tested on a Philippine airliner where a modified bomb was successfully smuggled on board the aircraft and exploded, killing one passenger. Had the broader plan been successfully executed, several thousand people could have died. Yousef's intended targets were not limited to the United States. Authorities also uncovered a plot to assassinate the Pope during his November 1994 visit to the Philippines.

⁷ This information was revealed in recently disclosed discussions between Mr. Yousef, the FBI and the Secret Service.

Whether the successful execution of these plans would have altered US foreign policy is in question. But the resolve of some individuals or groups to try is without doubt. Further, their methods prove difficult to detect and deter. Even with information gained from arrests following the World Trade Center bombing, detaining the leader of this group took years.

Aum Shinrikyo. The Tokyo subway event in 1995, involving the release of the chemical agent sarin, represents a third class of motivation – the desire to create chaos for political purposes. In this case, it was to bring down the existing Japanese government and install a new government. The events that took place seem simple, but the organization behind them is surprisingly large.

In June 1994, sarin was sprayed from a truck, killing 7 and injuring 200 people in Matsumoto, Japan. The motive and organization of the attackers was not understood until nearly a year later when, in March 1995, sarin was released in seven locations in the Tokyo subway system. This attack killed 12 and injured 5,500. Though a dramatic event as executed, the sarin did not disperse as planned, or casualties could have neared 10,000, as shown in Figure 4. That same month, the group also attempted the assassination of Japan's National Police Chief. Plans for attacks in the United States in Disneyland and against petrochemical facilities in Los Angeles existed as well. It was later learned that the group released anthrax in Tokyo on two separate occasions with no resulting casualties.

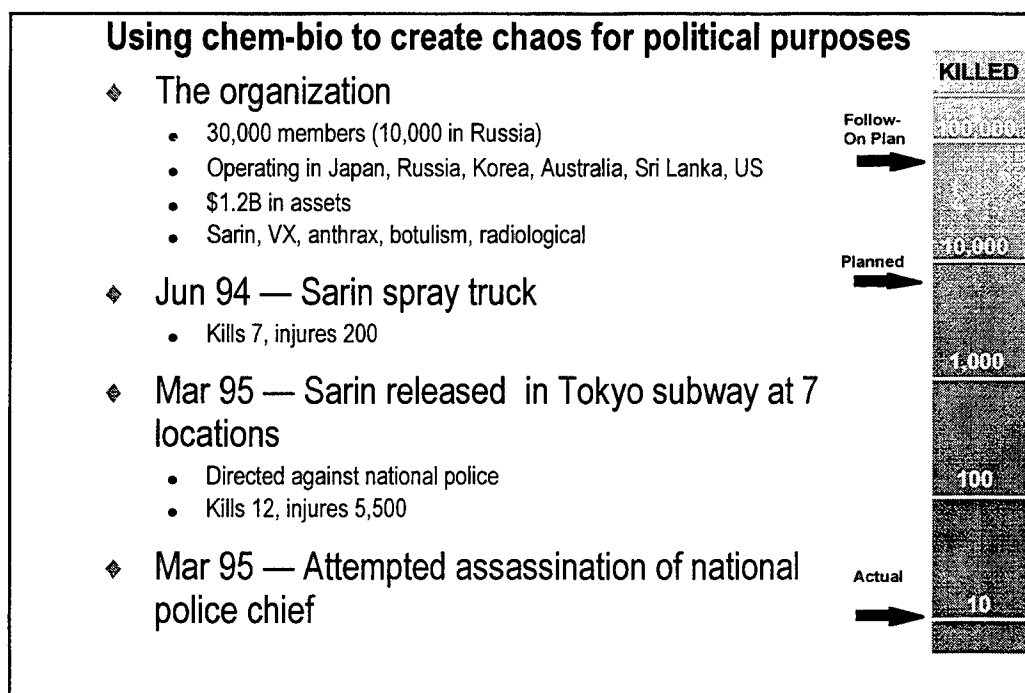


Figure 4. Aum Shinrikyo

The group behind these events had impressive membership, size, resources, and capabilities. With 30,000 people involved – 10,000 of whom were in Russia – this group resembled a small nation. It operated in Japan, Russia, Korea, Australia, Sri Lanka, and the United States with an asset base estimated at \$1.2 billion. The group had independent capabilities to produce sarin, VX, anthrax, botulism, and radiological weapons. Aum Shinrikyo still exists today in Japan and perhaps elsewhere. They are actively recruiting members, raising money, and organizing as before. More important, they are likely to have learned lessons from their past failures to achieve planned results.

The different types of motivation, consequence, and style of the transnational threat are evident from the three cases described. The capability for a few individuals or groups to produce major damage and loss of life exists today. Events that we have already witnessed could well have resulted in far graver consequences had they been executed with better precision or more effective agents. Figure 5 compares the potential impact of several such scenarios with the actual consequences.

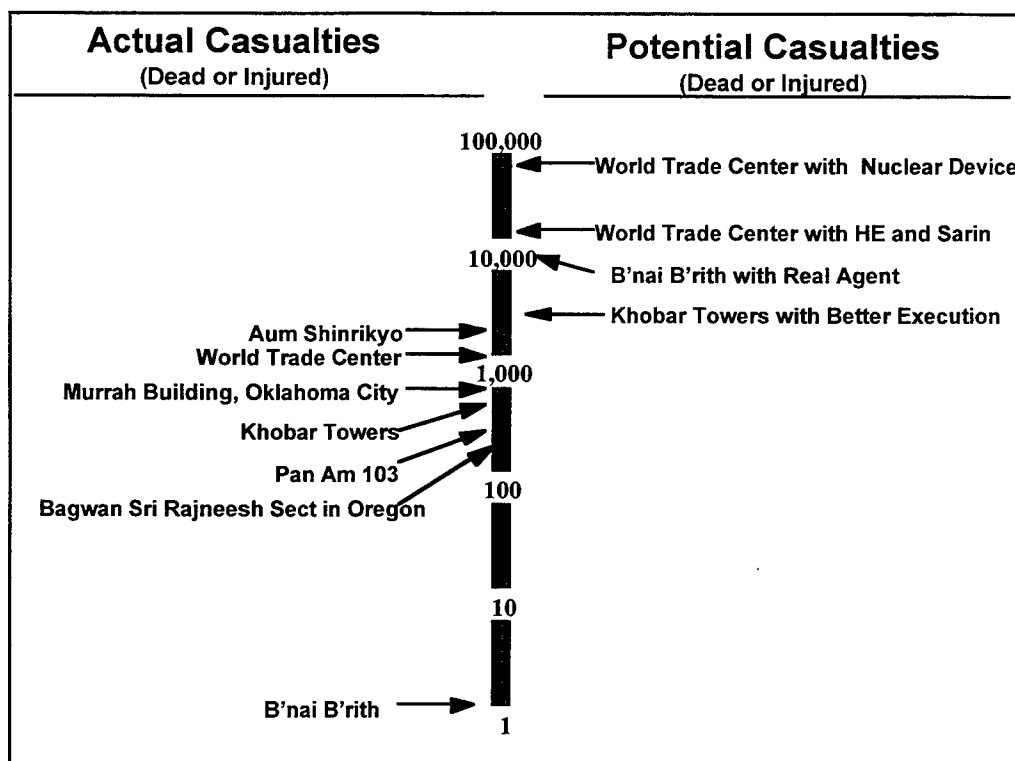


Figure 5. Potential Consequences of the Threat

A closer look at the April 1997 B'nai B'rith incident in downtown Washington, DC, is instructive. A package initially believed to contain anthrax was received at the B'nai B'rith headquarters. Later, the naval laboratory in Bethesda, Maryland, identified the contents as harmless bacteria and the incident was deemed a hoax. Nonetheless, several blocks of Washington, DC, had been cordoned off, B'nai B'rith personnel quarantined, and the two employees handling the package underwent decontamination procedures and were transported to

area hospitals. While no injuries occurred directly as a result of the package, had this been an actual release of anthrax, the outcome would have been vastly different.

Lawrence Livermore National Laboratory analyzed the incident and projected the outcome had there been an actual release of 150 grams (5 oz) of anthrax on the headquarters lawn from an aerosol can. Their estimates showed that based on prevailing winds, the cloud of anthrax would have contaminated the B'nai B'rith headquarters and dispersed to cover the White House and much of the Mall area, extending to an area over 30 square kilometers in size. Casualties would have been in the thousands, with fatality rates ranging from as much as 50 percent near the source of the release to 5 percent in outlying areas where concentration of the agent would have been lower.

The successful execution of scenarios of this sort could substantially impact America's sense of security, undermine public order, and instigate further incidents if the United States were unsuccessful in responding effectively. Furthermore, the consequences could extend internationally, eroding America's leadership position in the world community, limiting its ability to achieve foreign policy objectives, and directly impacting performance of military missions.

A Priority for DoD

Today, most US experiences have, or appear to have, involved isolated events or limited campaigns. But around the world, cases of multiple events, some of them quite serious, are prevalent. At this level, the threat can serve to limit DoD options or constrain operations and can have a serious impact on the economy and national cohesion. But if a transnational actor or nation state successfully waged an orchestrated campaign of these sorts against the United States, it could lead to mission failure, disengagement from overseas missions, and possibly national upheaval. America's position in the world could be altered. Figure 6 serves to illustrate the potential consequences of the evolving threat.

The task force believes there is evidence that the transnational threat will escalate in the future and that the threat will be dealing with extensive campaigns and greater use of weapons of mass destruction. The Libya retaliation campaign, the World Trade Center bombing, and the Aum Shinrikyo subway sarin release are examples of incidents that were part of an orchestrated, longer-term "campaign" which went unrecognized at the time these events unfolded.

US presence, policies, and leadership will remain a major stabilizing force in the world, which will require a range of credible offensive military capabilities, forward military presence, surge capabilities, and independent or coalition operations. A credible future global model depicts an environment that will require an activist foreign policy to sustain world stability, continuing foreign presence, and occasional military interventions in areas of conflict. This same model exacerbates stresses that traditionally motivate transnational threats. Thus, the transnational threat to the United States and its citizenry will become more significant over time.

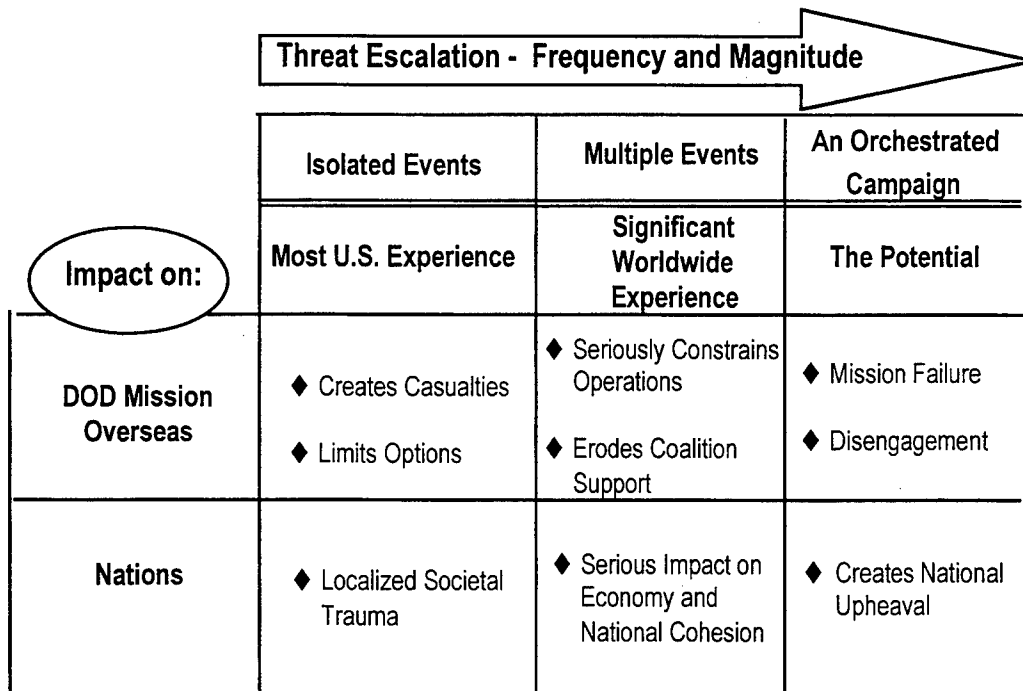


Figure 6. Threat Evolution

At the same time, US military operations will be subject to a growing list of vulnerabilities. All phases of combat operations, mobilization, logistics, command and control, engagement, and cleanup have become more dependent on communication and information systems which are susceptible to threat information operations. There will be fewer logistic sea and air points of departure and delivery in support of major military operations, which will make departure points more attractive targets for attacks using weapons of mass destruction. Many future military operations will be in urban areas and require contact with host populations – conditions at odds with typical force protection practices and capabilities.

Major military conflicts and transnational threats differ both in character and consequences, but do not differ substantially in the seriousness of the potential consequences, as Figure 7 depicts. It could be argued that many of the uncertainties associated with the transnational threat – the element of surprise, the difficulty of attribution, unclear purposes, and the possibility of attack on US soil – make it at least as challenging to counter as major theater war, and thus equally deserving of high priority within the Department of Defense. Moreover, the potential for significant casualties, in numbers far more than the public has experienced in recent regional military conflicts, demands that the problem be seriously addressed.

Major Military Conflicts

- Imminence of action normally detected and degree of response underway, if not prior, at least by commencement of hostilities
- Vital US interest at stake which results in direct US intervention
- Nation committed to war with another State
- Purpose of commitment clear in public's eyes and usually widely supported
- Unlikely that US soil attacked; combat casualties normally explainable and tolerated
- Military campaigns usually contained and lead to a decisive conclusion
- Coalition partners often join due to coincidence of interests

Major Transnational Threat Action

- Potentially low signatures; often a total surprise to leadership and casualties
- Significant US casualties lost and/or vital US capability destroyed
- Nation may not have a target to attack; possibly seen as impotent
- Purpose of attack may be unclear and difficult to explain
- Risk of attack on US soil both likely and becoming more easily carried out
- Unanswered actions may lead to additional "copycat" actions by other transnational groups
- Reluctance for other nations to become directly involved; seen as internal matter or cost of involvement seen as too risky (becoming target also)
- Success of persistent or pervasive actions likely to necessitate restrictions of democratic freedoms and individual liberties

Figure 7. Major Military Conflict vs. Transnational Threats

The task force recommends that to effectively counter this escalating threat, the President must raise the national consciousness across the government – at the federal, state, and local levels – as well as with our principal allies and coalition partners. In turn, the Department of Defense must treat countering transnational threats as a major DoD mission, with the same emphasis as major military conflicts. This involves including transnational threats in departmental guidance and strategy, in the planning and budgeting processes, and in training and exercises. This is not a new mission for DoD, but a different and difficult challenge to the traditional mission.

Recommendation: Treat transnational threats as a major national issue and major DoD mission.

- ⇒ The President must raise the emphasis on countering transnational threats, both in DoD and across the government, extending to the state and local levels.
 - ◇ A proactive interagency organization and process that exercises and tests the interfaces between federal, state, local, and international elements is needed.
- ⇒ The Secretary of Defense must treat countering transnational threats with the same emphasis as major military conflicts.
 - ◇ Focus in the Defense Guidance.
 - ◇ Define as an element of the National Military Strategy.
 - ◇ Focus planning and budgeting processes to ensure strong operational capabilities, including training and exercises, operational concept development, and new equipment.
 - ◇ Institute "red teams" to examine DoD efforts from the view point of the adversary and to measure progress against "world class" transnational threats.
- ⇒ The Secretary of Energy should commit to a corresponding mission emphasis in the Department of Energy.

Existing Structures and Processes

The transnational threat challenge requires a “three-tiered” response, as illustrated in Figure 8:

- 1) A *global response*, for international concerns, that is supported by a strong body of international policy, agreements, cooperation, and trust.
- 2) A *regional response*, in which the regional Commanders-in-Chief have primary responsibilities, including force readiness and force protection measures against both national and transnational threats. Interaction with coalition partner nations is critical.
- 3) A *force level response*, which focuses on force protection as a fundamental readiness mission requirement across the spectrum of threats.

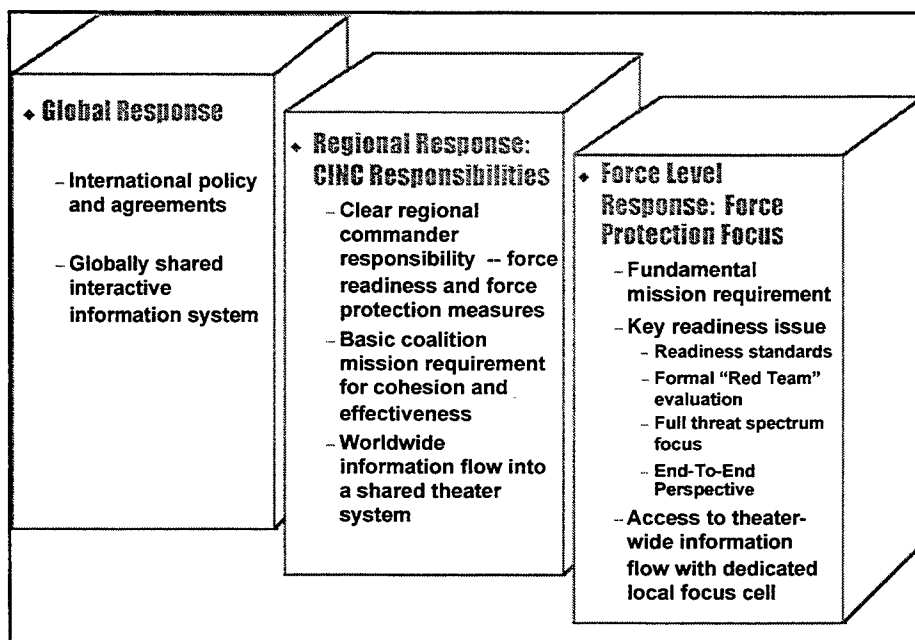


Figure 8. Three-Tiered Response to the Transnational Threat

Underlying all levels of this tiered response is a shared information system, described in the next chapter, that has reach from the global level, to theater-wide information sharing, to information flow dedicated to a local unit. Such a capability is essential to allow all users access to the information they need, from all available sources. It gives users at each level the opportunity to access and tailor information to meet their particular needs, to make adjustments as needs change over time, to provide information derived locally to higher authorities, and to access the wide variety of global collection assets.

This three-tiered response should capitalize on the parallelism between domestic preparedness, local force protection, and a major theater war. There is a strong synergy between the demands of force projection, force protection, and civil protection, as depicted in Figure 9. A robust force protection capability is critical to meet US security needs and maintain the nation's

ability to project its forces abroad. It is part of full-dimensional protection for US forces and extends to family members, civilian employees and facilities. Force protection also extends to installations, ports, and airfields in both the United States and overseas.

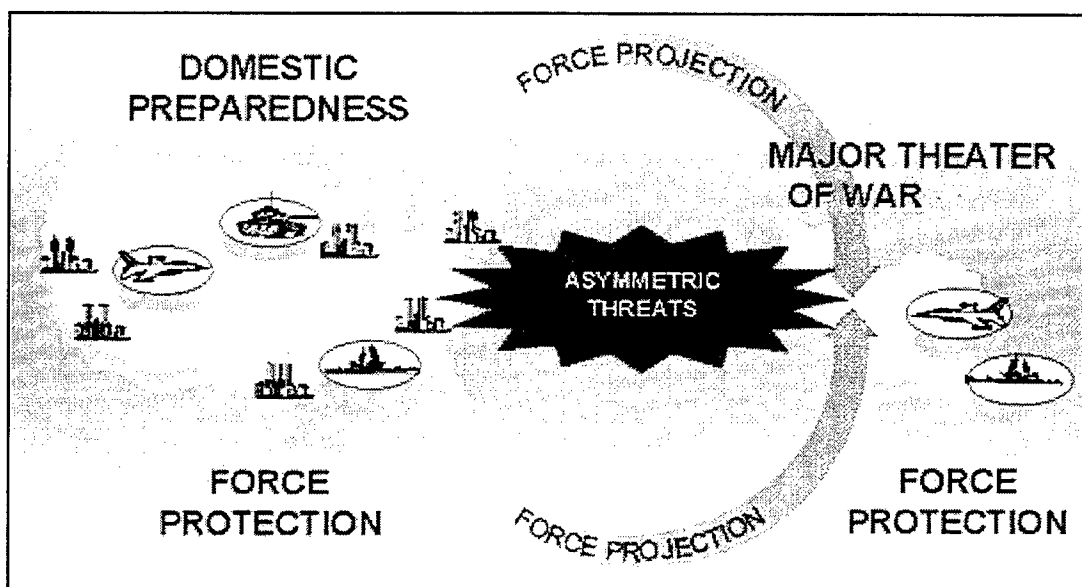


Figure 9. Linkages Between Force Projection, Force Protection, and Civil Protection

When closely examined, the requirements for protecting military facilities against attacks by transnational adversaries have much in common with protecting civilian facilities and people in metropolitan areas. This allows the United States to leverage DoD capabilities and expertise for both force protection and to assist in civil protection. There is a vast experience base in the civilian community among first responders – the firefighters, emergency medical personnel, and law enforcement officers who are first on the scene in the event of a crisis. And the existing resources and experience in DoD to cope with the battlefield use of weapons of mass destruction provide another experience base from which to draw. A more detailed look at each area serves to underscore these linkages.

Force Protection

Force protection is a major mission responsibility for the Department of Defense, for its forces at home and abroad. Responsibility for force protection rests on the shoulders of each regional and local commander. The Department is improving its force protection programs, and the findings of the initial vulnerability assessments – conducted by the Defense Special Weapons Agency on behalf of the Joint Staff – point to areas where improvements can be made.⁸

⁸ Volume II contains an expanded discussion of the force protection mission, the current force protection program, and task force recommendations.

These early assessments have shown that, despite efforts to elevate the importance of force protection, some apathy remains. Further risk mitigation measures may at times come at the expense of mission requirements and/or quality of life. Deficiencies exist in training and equipping security personnel, and in some situations, in physical security and protection against blast. Notable shortfalls also exist in capabilities for chemical and biological attack detection, characterization, warning, and mitigation. Personnel are particularly vulnerable in transit from one installation or post to another. In addition, in many posts overseas, US personnel are heavily reliant on host nation, third country, and contract labor which can raise unique security concerns. Moreover, overseas rules of engagement can be restrictive, thus limiting the influence of US forces outside the base perimeter. There is a need for local, organic, tactical intelligence collection and fusion capabilities that bring together information specifically relevant to addressing unique force protection challenges in specific locations.

The Secretary of Defense should reemphasize force protection as a mission responsibility by elevating its priority in departmental strategy and guidance. The task force believes that DoD in general, and the Chairman of the Joint Chiefs of Staff in particular, deserve high marks for the force protection efforts to date. But the problem has not yet been fully addressed, and there is still much to do. An enhanced force protection program demands: an end-to-end mission orientation, expanded vulnerability assessments, patching the "seams" created by diverse responsibilities, focusing intelligence programs and capabilities, and exploiting promising technologies, including the creation of a test bed focused on force protection.

The Department can further exploit current and emerging technologies to reduce force protection vulnerabilities. The task force believes that there are a substantial number of unexploited technologies that can be employed to enhance force protection capabilities both in the near-term using commercial, off-the-shelf products and in the long-term as various new technologies mature.

One promising new technology is the force protection "associate" – a collection of integrated software tools for facility vulnerability analysis and risk management modeling that can be used by local commanders. This tool could aid in deconflicting intelligence data and relating such data to that drawn from local monitoring sources. It could also manage a local area intelligence/surveillance system and provide for information sharing among different people in different situations. DARPA is examining this concept for possible development.

With the many ideas available from both DoD labs and private industry, an issue is how to prioritize and exploit these technologies to ensure that they make a difference. A screening process is needed to help evaluate the technology options and accelerate the deployment of promising technologies. A force protection test bed that involves the users in the evaluation process would serve such a function and have the added benefit of sustaining the necessary focus on force protection as a continuing effort. The task force recommends that the force protection test bed initiative be assigned to the Joint Forces Command, as proposed in the Report of the National Defense Panel, or should DoD not establish this organization, to the Atlantic Command.

The Task Force recommends an initial investment of about \$10 million per year. The following chart summarizes the key force protection recommendations.

Recommendation: Force Protection needs new emphasis.

- ⇒ DoD should elevate the priority of force protection plans and programs – in the departmental guidance and in the requirements and budget processes.
- ⇒ The Chairman should expand the scope and breadth of vulnerability assessments.
 - ◇ Include people, mission, infrastructure, and lines of communication
 - ◇ Expand biological, chemical, radiological, and nuclear considerations
 - ◇ Make inspection-like – with compliance monitoring at all levels
- ⇒ DoD must adopt an end-to-end, systems engineering approach to rationalize policy, plans, programs, and budget.
 - ◇ Develop a plan to demonstrate and field integrated force protection systems
 - ◇ Develop a rapidly deployable force protection augmentation capability
- ⇒ Enhance intelligence operations for force protection.
 - ◇ Focus more on timely, correlated warning
 - ◇ Add organic tactical intelligence capabilities to overseas units
- ⇒ Pursue science and technology initiatives, through development and implementation by the Services and DARPA.
 - ◇ Develop a joint force protection test bed established by the Joint Force Command or USCINACOM
 - ◇ Develop a force protection “associate” to support local commanders, using DARPA

Taking these steps will help the Department emphasize force protection as a “state of mind” and a constant way of life. It is this focus on “state of mind” that is necessary for DoD’s force protection efforts to be truly effective.

Civil Protection

Similarly, civil protection begins with the state and local first responder community – law enforcement, fire and rescue, medical, and emergency management personnel. Depending on the severity of a crisis, as shown in Figure 10, federal assets may eventually become involved. Both the Department of Defense and the civilian community can benefit from improving the integration between the state, local, and federal agencies. Improvements in communication, training, information sharing, operations, and resource transfers would help to streamline emergency response operations and interfaces across all levels of responders. Also, utilizing the National Guard more effectively in their state, and in some cases their federal, role can serve to strengthen the linkages between civil protection and force protection with benefit to all participants.

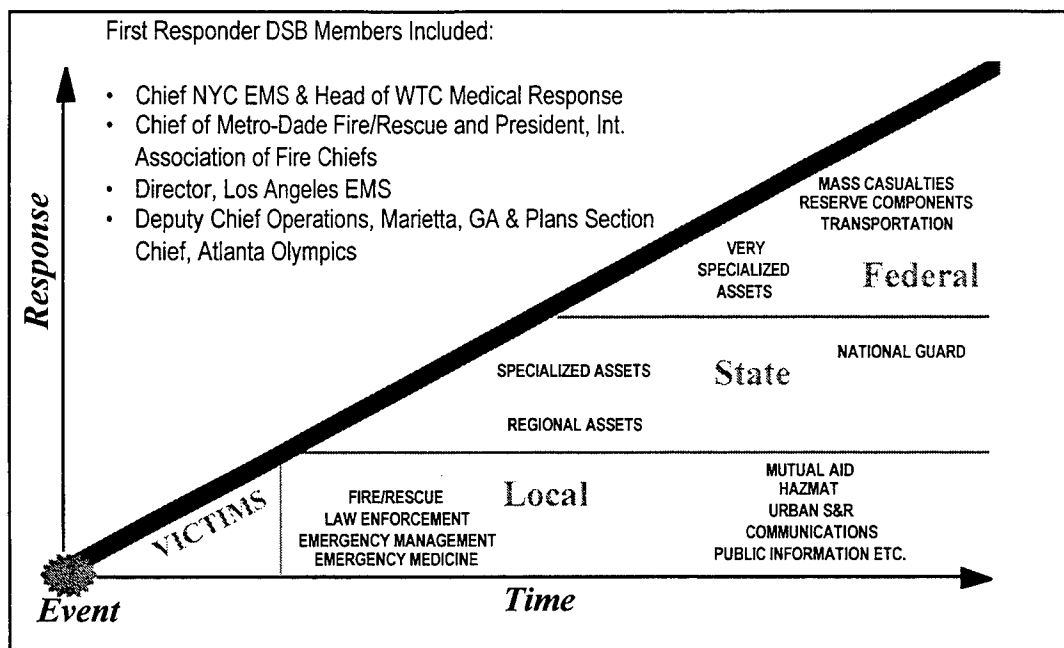


Figure 10. Challenges and Players in Consequence Management

The Department of Defense is assigned a wide and complex set of responsibilities to support civil protection under a variety of statutes, from prepositioned response capabilities, to crisis preparation and management, to consequence management. The Department has a role in both maintaining readiness and in planning, coordinating, and executing crisis response.

Among DoD's assets, Army and Marine Corps chemical units have personnel trained in protection, detection, decontamination, and cleanup and have specially tailored equipment. DoD response assets also include a variety of research and training institutes with a core of subject matter experts that can supply needed expertise and first hand experience.

The Nunn-Lugar-Domenici Amendment on Domestic Preparedness was enacted by Congress in fiscal year 1997, to *enhance the capability of the federal government to both prevent and respond to civilian incidents*, particularly those involving weapons of mass destruction. The law also provides resources aimed at *improving the capabilities of state and local emergency response agencies* to prevent and respond to such incidents at both the national and local levels. The law recognized the current gaps that exist in the national capability to respond to terrorist incidents involving weapons of mass destruction. Under this law, DoD was directed to provide emergency response training, advice, and assistance to first responders; assist in developing a rapid response team; conduct testing and evaluation of preparedness; assist in developing and maintaining an inventory of physical equipment and assets; and assist in procuring equipment to interdict weapons of mass destruction.

Figure 11 shows the spectrum of new initiatives that are funded under Nunn-Lugar-Domenici, beginning with interdiction and continuing through response. Training activities are underway, as are plans for exercises to test integrated response plans. Procedures for loaning equipment are being put in place. Eventually there will be resources such as a hotline, helpline, and web page where state and local authorities can seek advice and access to expertise resident outside of the local jurisdiction. Data bases and list of inventories will also be available to support crisis response and planning. In fiscal years 1997 and 1998, the Department of Defense received \$84.7 million in funding to support these activities.

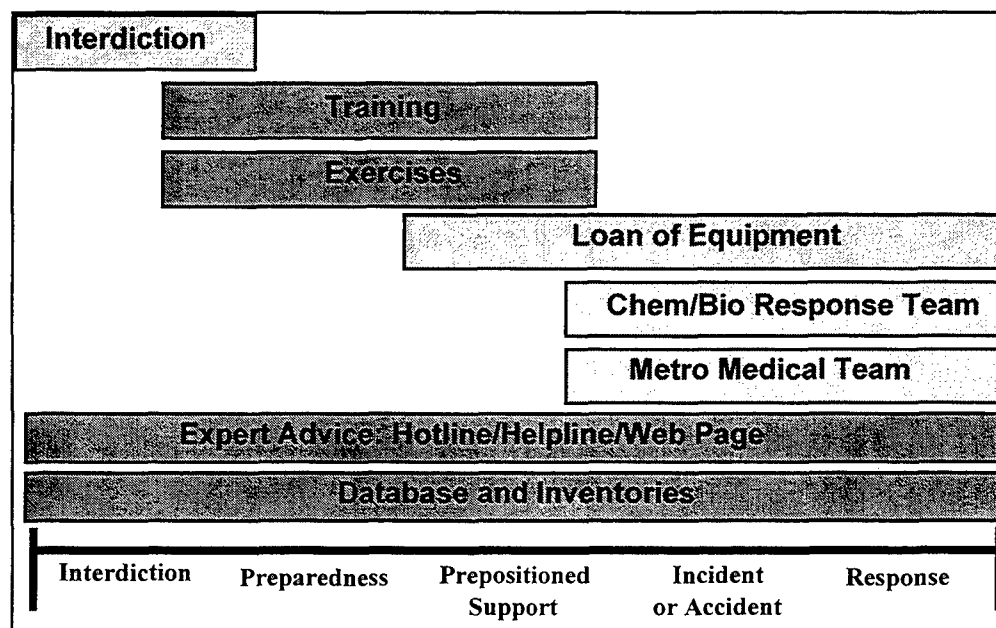


Figure 11. Spectrum of Nunn-Lugar-Domenici Support

The task force recommends that DoD improve its capabilities to support civil crisis response and consequence management. The first step involves developing a plan to expand the scope of Nunn-Lugar-Domenici and institutionalizing it within the Department. Readiness must be a continuing effort and resources must be dedicated. There are currently plans for the Nunn-Lugar-Domenici program to continue in the hands of the Federal Emergency Management Agency, but the task force believes that an enhanced program within the Department of Defense is needed to bring together the assets of both the civilian and military communities.

DoD's leadership in helping prepare for the domestic terrorist threats will have an immediate positive impact on its core mission of maintaining force protection in the military. Further, the synergy between DoD's efforts in force protection and support to domestic preparedness will put in place a more effective consequence management and mitigation structure.

The task force concludes that the National Guard should play a more central role in DoD's support to civil protection. The Guard is involved in most significant incidents today and is associated with local emergency and law enforcement communities, with long term expertise.

Some Guard members are themselves also first responders. The task force sees two enhanced roles for the National Guard to make them more fully effective in the complex incidents possible in the future. First, *provide a national consequence management capability, within the framework of Title 32 and Title 10, to increase DoD's support to state and local agency responses to domestic incidents of all types, but with particular emphasis on chemical or biological incidents.* Second, *support sustainment training and exercises for first responders for cases involving chemical or biological agents.* In addition to assisting in domestic consequence management, if necessary, these capabilities can also be utilized to provide similar consequence management augmentation to the regional combatant commanders when appropriate.

An integrated state and regional National Guard capability would consist of both state rapid assessment teams and regional chemical-biological incident response units. Together, these teams would require 4,000 National Guard personnel, which represents only about one percent of the National Guard structure. To equip the teams, the Assistant to the Secretary of Defense for Nuclear and Chemical and Biological Defense Programs should evaluate and recommend appropriate equipment for National Guard consequence management response.

These state teams, modeled after the Marine Corps Chemical Biological Incident Response Force, would augment first responders by providing a rapid reaction capability for initial decontamination and medical assistance. The teams would integrate into the existing First Responder Incident Command System – the first responder command and control system – as well as integrate with Federal Emergency Management Agency regional offices and appropriate state and local agencies. The state units would also participate in exercises and training across this spectrum of agencies.

Recommendation: Improve DoD capabilities for support to civil response and consequence management mission.

- ⇒ The Secretary of Defense should direct the Army to develop a plan to expand the scope of and institutionalize the Nunn-Lugar-Domenici program. The Department should retain DoD stewardship of this program to:
 - ◇ Fund development and operation of a Global Interactive Information Network
 - ◇ Expand training to include distance learning centers coupled with modeling and simulation, and use the National Guard to train the trainers and for support in general
 - ◇ Expand the Nunn-Lugar-Domenici program in the Army budget to \$200 million annually beginning in the fiscal year 1999 program budget
- ⇒ The Secretary of Defense should direct the Army and the National Guard Bureau to establish a national consequence management capability to support state and local agency responses to domestic chemical and biological incidents, and support the regional combatant commanders' consequence management Joint Task Force.
 - ◇ Startup cost estimated to be \$320 million over 3 years; sustainment costs \$70 million annually

No New Organizations

DoD can and should respond to the escalating transnational threat challenge using the existing national security structure and processes. While it may be necessary to set up a special interagency group to plan and coordinate across the government responsibilities, DoD's internal responsibilities emanate from the fact that the transnational threat is a core, cross-cutting DoD mission. That mission can and should be addressed within the structure that plans for and executes the other core, cross-cutting DoD missions.

Each of the military departments have work to do to organize, train, and equip to focus on this threat. This area has unusually broad policy implications and needs. While the task force has suggested some out-of-the-box technology efforts, these efforts and the rest of the acquisition activities fit well within the core acquisition structure of DoD. The joint operational concept and architecture task is a task for the Joint Staff, specifically J-8 and J-3. Virtually all the other Joint Staff elements will have work to do that is not that different in character from work associated with other missions. Every Unified Command will have focused work to do to plan for and carry out this mission.

In contrast, creating a special agency could be counterproductive in that the broad range of DoD activities that need to focus on this mission could be inclined to leave it to the special agency.

Within the existing structure, the Secretary of Defense should clarify responsibilities throughout the organization for policy coordination, operations, and research and development. Currently, multiple offices within the Department are involved with no one office effectively positioned to ensure that DoD's posture is effective against the transnational threat.

Responsibilities for antiterrorism, counterterrorism, arms control, transnational threats, infrastructure protection, and force protection are distributed across several offices in the Office of the Secretary of Defense and in the military services. For example, capability building in response to the nuclear, biological, and chemical threat is the responsibility of the Assistant to the Secretary of Defense for Nuclear and Biological and Chemical Defense Programs (ATSD[NCB]), the Defense Special Weapons Agency, individual service programs, and several other offices within the Office of the Secretary of Defense. Both the National Security Agency and the Defense Information Systems Agency have programs to develop capabilities in response to the information warfare threat. The formulation and coordination of policy and strategy is led by the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict, the ATSD (NCB), and by the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (C3I).

Figure 12 provides an example of how new ownership and responsibility might be assigned within DoD. Here functions associated with nuclear, chemical, biological and conventional threats have been separated from those associated with the information warfare threat, with policy

oversight assigned to the Under Secretary of Defense for Policy and to the Under Secretary of Defense for Acquisition and Technology, respectively. At the operational level, the regional warfighting Commanders-in-Chief are given responsibility for both crisis management and consequence management. Specifically SOCOM and USACOM are assigned to crisis management; USACOM is assigned to consequence management within the continental United States and the appropriate regional commanders are responsible in cases occurring abroad.

<i>Function</i>	<i>Policy Oversight</i>	<i>Operations</i>	<i>Operational & Systems Architectures</i>	<i>R&D Oversight</i>
<i>Nuclear, Chemical Warfare, Biological Warfare, and Conventional Threats</i>	USD (P)	SOCOM and USACOM for crisis management Area CINCs for consequence management; USACOM for CONUS	JCS Task Force and USD (A&T)	DDR&E, supported by ASD (SO/LIC) for crisis management and USD (A&T) for consequence management
<i>Information Warfare Threats</i>	USD (A&T)	Appropriate CINC		DDR&E

Figure 12. Example of Ownership Within DoD

The task force proposes a temporary Joint Task Force, within the Joint Chiefs of Staff organization, coupled with a team assigned by the Under Secretary of Defense for Acquisition and Technology, to design operational and systems architectures. Research and development oversight is broadly assigned to the Director, Defense Research and Engineering, and supported by the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict in the area of crisis management, the Office of the Under Secretary of Defense for Acquisition and Technology in the area of consequence management.

Recommendation: No new organizations.

- ⇒ The Secretary of Defense must assign responsibility for transnational missions with greater clarity than exists today.
- ⇒ The Secretary of Defense must clarify and assign, to a single policy office, responsibilities for counterterrorism, counterproliferation, transnational threats, and infrastructure protection.
- ⇒ The Secretary also must assign responsibilities for the National Guard in the area of civil training, exercises, consequence management, deterrence, and regional combatant commander consequence management support in chemical and biological warfare incidents.
- ⇒ The Chairman of the Joint Chiefs must assign responsibilities for
 - ◇ Updating all operational plans to include transnational threat contingency planning, crisis response and consequence management responsibilities
 - ◇ Budgeting by the Services for new transnational threat requirements derived from Joint Task Force outputs in the program period beginning in fiscal year 1999
- ⇒ DoD must also work cooperatively with the Department of Energy to develop an expanded memorandum of understanding and research and development plan to address transnational threats.

Structuring the Operational and Technical Architectures

The elements necessary to respond to the transnational threat exist within the Department of Defense, as does the expertise. But DoD needs a more comprehensive plan. These varied and diverse elements need to be refocused and woven together into a cohesive, strategic response to the transnational threat – a response that effectively leverages all available resources within the Department.

Both operational and technical architectures are needed to focus the numerous activities and responsibilities needed for a coherent DoD approach to meeting the variety of transnational threats. This set of threats is distinctly different than the conventional threat set while demanding the same level of attention as conventional threats that motivate capabilities to deal with major theater wars.

The challenges include:

- Collecting information from a very wide set of sources
- Providing intelligence on a wide set of threats
- Formulating approaches to deter and defeat threats to forces worldwide; the means to deploy forces worldwide; the host nation support needed for successful coalition operations; and public support for contingency operations, from both the United States and host nation populations
- Equipping and training appropriate segments of the force for the special challenges posed by transnational threats
- Exercising and testing the readiness of these segments of the force
- Commanding and controlling these forces across a wide spectrum of employment possibilities

The Joint Air and Missile Defense Office (JTAMDO) provides a useful existing model for formulating such a cross-cutting operational architecture. While in many respects the JTAMDO task is somewhat easier to define than the transnational task, JTAMDO is creating a coherent joint operational architecture for a broad mission area that has been badly needed for several decades. The corresponding effort to produce the supporting joint technical architecture is less mature and may be less relevant to the transnational threat. In the case of air and missile defense, a joint agency, the Ballistic Missile Defense Office, has the responsibility for the technical architecture. For the transnational threat, it is likely that several technical architectures will be needed – for information and intelligence; for force protection; for command, control, and communications; and for civil integration among others.

As noted earlier, the problems and possible solutions associated with the transnational threat cut across many missions and organizations in the Department of Defense. Numerous existing efforts deal with a part of the problem or part of the solution, or have overlapping

responsibilities. And information is not readily available to others to whom it might benefit. Moreover, the information flow between DoD and other government agencies who are also committing resources to the transnational threat must be improved. DoD must develop a concept of operations that encompasses the entire range of missions involved in the threat response – an “end-to-end” system-of-systems design that incorporates the requirements for deterrence, detection and interdiction, prevention, consequence management, attribution, and response.

The task force recommends that the Department develop an architecture defining an end-to-end operational concept and a system-of-systems structure. This architecture must define the interfaces between crisis management and consequence management to ensure there is no gap. The plan must identify technology needs and requirements and must identify priorities for research and development, acquisition, exercises, training, and “red teaming” to provide a sound basis for an investment strategy. Furthermore, this architecture must chart evolutionary paths with options to ensure that the United States keeps pace with the threat. Tools such as models, simulations, and analytical expertise should be used to continue and enhance the process over time. The value of such planning efforts far outweigh the estimated cost.

Recommendation: Develop an architecture defining an end-to-end operational concept and a system-of-systems structure.

- ⇒ The Chairman should establish a temporary Task Force in the Joint Staff to develop operational and systems concepts and a Master Plan. The initial deliverable from this group should be due in six months.
- ⇒ The Under Secretary of Defense for Acquisition and Technology should establish a temporary joint Technical Support Team that will provide a systems architecture, and exercise support, modeling, and analysis capabilities to assist in the development of the system-of-systems structure and Master Plan.
- ⇒ The approach should:
 - ◇ Use red teams extensively to emulate responsive threats
 - ◇ Exploit modeling and simulation to test and evaluate alternatives
 - ◇ Strongly emphasize exercises and tests – not just paper studies
 - ◇ Develop separate but interactive initiatives for force protection and civil protection
 - ◇ Be complete in 18 months
- ⇒ Cost: \$30 million over 18 months.

CHAPTER 3.

Technical Challenges

"There is now greater danger of nuclear attack by some outlaw group than there was by the Soviet Union during the Cold War."

DIRECTOR, FEDERAL BUREAU OF INVESTIGATION, LOUIS J. FREEH

CHAPTER 3. TECHNICAL CHALLENGES

A Global Information Infrastructure

The United States must get smarter about transnational threat groups – their motives, organization, sources of support, and operational means. As such, there is a need for an interactive, two-way global information system that would expand the available sources of information. This system would support gathering more data from the bottom up, exploiting international information sources, and two-way sharing of critical information with state, local, and international partners. It is also important to do net assessments on the transnational threat and US responses – to look at long-range moves, countermoves, and capabilities, and to evaluate US response capabilities over time. An analytic framework and better analytical tools are needed for planning and assessing the effectiveness of capabilities to gather, process, and disseminate information about these threats.

The task force was sensitive to privacy issues in formulating recommendations on global information. These recommendations do not call for more intrusive information sources. They are, instead, intended to focus existing data bases and information on the transnational threat.

The World Trade Center transnational threat campaign is an example of how better sharing of information between federal, state, and civilian agencies might have prevented the bombing of the tower. The task force believes that sharing and correlation of information could, in fact, help to prevent and even deter future transnational threat activities.

At the present time there are no formal processes, infrastructure, and security mechanisms to facilitate the sharing and analysis of transnational threat information collected by organizations such as local law enforcement, National Guard, Immigration and Naturalization Service, Department of Energy, Central Intelligence Agency, Federal Bureau of Investigation, the Department of Defense, and other organizations. Individually, these organizations collect data that, when viewed independently, may not provide knowledge about plans for an activity or campaign by a transnational adversary. However, correlation of diverse data sources would likely enhance our ability to identify key indicators and provide warning.

Furthermore, other sources of data that could be exploited to provide indicators and warning of transnational threat activities largely remain underutilized. Examples of such sources include the real-time data on international border crossings, real-time cargo manifests, global financial transactions, and the global network carrying international airline ticket manifests. Technology initiatives can support the use of needed data. New techniques such as bio-markers to detect

antibodies that might point to the location of threatening activities, “sticky paper electronics” for covert sensing and tagging, and nano-robots for covert sensor deployment need to be examined.⁹

If the United States decides to share available information technology, new data sources could be integrated using a tiered security architecture. Tapping into selected US and international data bases, it would be possible to develop a much better global information system that would permit timely, collaborative analysis and correlation of information on transnational groups. This infrastructure would augment each contributing organization’s ability to pursue its specific mission and would be a tool whose specific purpose is to facilitate the acquisition, sharing, and collaborative analysis of data that will provide improved knowledge about emerging transnational threat groups and their activities.

Such a two-way distributed information system – which the task force termed the Secure, Transnational Threat Information Infrastructure (STII) – can be at least started with information technology and relevant data bases that exist today. These technologies include data communications infrastructure; distributed, relational data base systems; emerging multimedia data base technology; computer-network security hardware and software; and use of the World Wide Web. In addition, significant public and private sector investments are being made in research and development of advanced information technologies to include data mining, data warehousing, intelligent agents for information fusion, intelligent data base triggers, and groupware to support distributed collaboration among analysts.

As public and private sector advanced information technologies mature, the baseline system would be augmented so that the correlation and fusion process becomes more automated, more tools are provided to facilitate distributed collaboration, and dynamic security techniques are integrated to permit various communities of interest to participate in transnational threat warning, deterrence, and prosecution activities. The task force anticipates that as this two-way data gathering and distribution system evolves, it would serve not only as a means for obtaining indicators and warnings, but argues that its successful use would also serve as a powerful deterrent to threat activities.

An example of such an infrastructure that has been developed and deployed to successfully support counter-narcotics operations is the RIONET. This system, although of much smaller scale, proves how integrating information systems from multiple sources can be effective in supporting a broader mission.

Technology is necessary, but not sufficient, for establishing and realizing the benefits of an integrated, global information system. Strong, dedicated leadership that promotes the proactive use of the transnational threat information infrastructure, seeks necessary resources, and addresses inter-organizational data sharing will be required. This leadership must have sufficient authority to cause the integration of federal, civil, and international information systems. In

⁹ Annex C contains a detailed description of these and other technology initiatives.

addition, policy will have to be established that permits sharing of data between organizations with distinctly different missions, constraints, and security structures. A multi-tiered security structure will be required and huge cultural and institutional barriers will need to be broken down.

Policy, as well as procedures and mechanisms, will have to be set to allow meta-information to be acquired, developed, and used as indices into the many data bases that will comprise a global, distributed, transnational data base. One approach for acquiring this metadata is to actively solicit, reward, and filter information on transnational threat activities potentially available on the global internet. The mechanism for acquisition would be through the Global Information Infrastructure (GII) – more familiarly known as the World Wide Web – which today is an under exploited information-acquisition resource. Through the use of carefully designed, intelligent information-request forms, the correlation and fusion of data from multiple, disparate data bases within the system's infrastructure will be greatly facilitated. The development of metadata can also be automated through intelligent data mining tools under research today.

Not only does the World Wide Web provide a resource for information acquisition, it can provide the foundation technology and infrastructure for establishing an initial, operational transnational threat information and distribution infrastructure. The Web can be used as the wide-area backbone, or the data transport segment, of the system – interconnecting the data systems of the variety of agencies involved, many of which are already connected to the Web. With this approach, the STII would become a virtual, secure sub-network within the Web. This sub-network would be secured with multi-tiered security arrangements to prevent access by unauthorized users. The security boundary would be established at the transport, data base, and application layers, using both commercial and defense security technologies where appropriate including firewalls, public key cryptography, and digital signatures for data distribution.

An important attribute of the World Wide Web is that information flows freely across national boundaries. Although several nations are attempting to curtail, or manage, this information flow, attempts to do so have thus far been ineffective. As computer systems – from desktop to laptop to network-based systems – become more affordable, particularly in emerging nations, this resource will be even more accessible to the working-class and student populations in these countries. These individuals, and the Web itself, are potential sources of timely transnational threat information that cannot easily be accessed through other means.

Today the global information infrastructure is viewed more often as a vulnerability – it provides information freely, efficiently, and unaccounted for on many topics potentially useful to certain groups. This view loses sight of many potential benefits. Exploiting the Web provides insight into the type of information that is openly available to a potential transnational adversary, and allows for remote and anonymous participation in on-line “chat” forums that might provide insight into dissident group activities. The medium can be used to disseminate information worldwide and, as noted previously, can be used to solicit, judiciously, information which may be of value.

Although it is important to continue to address vulnerability, security, and information content issues associated with using the World Wide Web, it is also important to determine how best to use this resource as an information tool. Accepting the Web as a resource is not contradictory to concerns about its exploitation by an adversary, but instead takes advantage of a resource that does, and will continue to, exist and grow over time. The creative use of the Global Information Infrastructure and the employment of the STII are the basis for developing processes and procedures for collectively addressing the transnational threat across the defense, civil, and international communities.

Recommendation: Develop a new global, shared interactive information system.

- ⇒ The Secretary of Defense should direct the Under Secretary of Defense for Acquisition and Technology to develop the shared interactive information system.
- ⇒ The Secretary should request that the Director, Central Intelligence, the Departments of State and Justice, and the Treasury Department contribute technical and operational support and involvement in the development and operation of the STII.
- ⇒ Civil, state, and international involvement must be ensured via:
 - ◇ National Guard and reserves
 - ◇ Law enforcement community through the Department of Justice
 - ◇ Consequence management community through FEMA
 - ◇ Coalition nations and other allies through the Department of State
- ⇒ Schedule
 - ◇ The Department of Defense develops a plan for implementing the STII in the program budget period to begin in fiscal year 1999
 - ◇ Initial operational capability within the continental United States by 1999
 - ◇ Full operational capability worldwide by 2001
- ⇒ Cost
 - ◇ The startup cost in fiscal 1998 of the system is estimated at \$30 million, resources which could be available through Nunn-Lugar-Domenici
 - ◇ Total cost estimate is \$300 million for development and federal procurement
 - ◇ Operational costs are estimated at \$50 million annually

Addressing the "Too Hard" Problems

There are a number of challenges that have historically been regarded as "too hard" to solve: the nuclear terrorism challenge, defense against the biological and chemical warfare threat, and defense against the information warfare threat. This task force believes that these challenges should be addressed and incremental improvements should be sought and implemented; doing so will make a substantive difference. Against the nuclear challenge, sensor and information network technology improvements will permit better exploitation of threat signatures. Actions can be taken to first detect and then substantially limit the consequences of threats from both biological and chemical warfare. The task force also envisions adaptation by DoD of a defense-in-depth approach to mitigate the information warfare threat. Each is discussed in more detail below.

In thinking about options, the United States must avoid being trapped into any variant of "it's too hard" that will lead to inaction. Currently, cost-effectiveness relationships are not well understood for these threats, but such a situation is not without historical precedence. For example, it took the United States a decade of thought and debate from the late 1940s to late 1950s to develop fundamental strategies for nuclear deterrence and eventually the triad flexible response concepts for the strategic nuclear threat.

Another trap the United States should try to avoid is that effectiveness must be measured against only the most stressful threat and/or embrace only the perfect solution. In these cases, we will quickly find ourselves limited by either ideas or dollars (or both) while any investment made will produce a capability of limited effectiveness. Moreover, not dealing with these threats leaves the United States open to enormous consequences should a successful attack actually occur.

Alternative choices for effectiveness – such as minimizing people exposed or assets contaminated, raising the ante for the adversary such that he might show his hand, providing confidence to the public and our allies that we are serious about addressing the threat – lead us very naturally to a continuing effort to improve our capabilities to deal with the nuclear, chemical, and biological transnational threat. A technology need not be 100 percent effective to have significant deterrence value. Each incremental contribution can be important. A similar approach has been pursued, with obvious success, to drive down aircraft hijackings.

Selecting the steps and their sequence in a systematic way is highly recommended; in fact, it is consistent with the architectural approach recommendation contained within Chapter 2. While many things are happening in an ad-hoc manner to improve our capabilities, the analysis to identify the highest priority actions is not.

The Nuclear Challenge

If the required fissile material is available, it is not difficult to design and build a primitive nuclear explosive device. It is unlikely, though not impossible, that it could be done by just a few people. But because of the diffusion of knowledge and technology over the past decades, it no longer requires the resources of a nation state. It is more difficult to make weapon-grade plutonium or enrich uranium for such a device, but with the amounts of such materials in all the states of the Former Soviet Union and elsewhere, materials – or weapons themselves – might be obtained from these sources. Other sources are the growing stockpiles of spent nuclear reactor fuel stocked all over the world. This development over the last few years adds to the urgency of dealing with the nuclear threat.

A nuclear device could be small enough to be covertly transported to its intended detonation point by a small truck, ship, or an aircraft of moderate capacity, or perhaps a combination of transport means. Such a device, with yield about the same as the weapons used in 1945, could be

detonated in a city, at a military base in the United States or overseas, or against US or other forces in the field with devastating consequences. There is no way to assign a "likelihood" or "probability" to such an event.

Such an explosion could change the world. The tradition of non-use of nuclear weapons, developed since 1946, would have been broken. Attitudes toward nuclear weapons, and the roles they play in regional and global security relationships, could change dramatically, with unpredictable and possibly serious effects on those relationships. If used against US forces overseas, such an explosion could demonstrate a potent and asymmetric countervailing of US military capability, limiting the ability of the United States to use its military effectively in the many roles it plays around the world. If detonated in a city, the unprecedented vulnerability people would feel in their daily lives could lead to changes in political institutions and types of governments – in the social contract itself.

The possibility that such a nuclear device could be built and detonated has been understood for over thirty years and some good capabilities to search for and disable a stolen weapon or a covertly placed device have been developed. But these current capabilities cover only a very limited part of the range of possible future threat scenarios. Furthermore, there is not now, nor has there ever been, a comprehensive program to develop, even over the long term, a robust capability to combat this threat across a wide range of possible scenarios. There are several reasons for this, but in part it is because the problem has simply appeared to be "too hard," no matter what level of resources might be devoted to its resolution.

The task force believes that for costs far less than what would be commensurate with the possible consequences of such an explosion, and with a comprehensive long-term program, there is a good chance that capabilities can be developed to deal effectively with this threat – i.e., to cover, with good effectiveness, a much larger part of the range of possible threat scenarios. This is especially true when the dissuasion/deterrent effect of greatly improved but less-than-perfect protection capabilities is added. This belief is based on a combination of existing understanding and capability, some new realizations about parts of the problem and possible solutions, and prospects for new technical and operational capabilities.

To realize this potential, the task force recommends that the Secretaries of Defense and Energy should significantly expand their departments' efforts related to countering the transnational nuclear threat. Added to the current effort, which is largely devoted to current operations and readiness, should be a major program component that looks to the farther future, to develop a greatly improved capability. This development program should be based on the assumption that, as it becomes successfully complete, procurement and operational resources can then be made available which are much greater than those available today.

Even when this improved capability has been developed, maintaining the substantial assets involved at a high level of readiness may not be perceived to be affordable, either politically or fiscally. What *can* be done is to address the long-lead items – such as training, long-lead

procurements, and preparations to procure – that would be needed to surge rapidly and effectively, if and when circumstances develop that change perceptions of political or fiscal affordability. *Such preparations, starting now even with the limited capabilities that currently exist, should be an integral part of a comprehensive program.*

Of note, this study primarily focuses on DoD responses and capabilities, but the Department of Energy plays an integral part in dealing with the nuclear transnational threat. The discussion that follows addresses current and future capabilities without reference to the organizational boundary between the two departments. But this boundary exists. Finding the right way, in the DoD/DOE relationship, to gain the benefits of both close collaboration and independent views is an important and difficult issue that must be addressed.

An improved posture to defend against the nuclear transnational threat must tightly integrate many elements – information and intelligence, security of nuclear materials and weapons, threat device detection and disablement, consequence mitigation, and attribution. Each of these elements is discussed in the following paragraphs.¹⁰

The task force recommends that, within the overall architecture for responding to transnational threats, the Departments of Defense and Energy should jointly develop a comprehensive, end-to-end architecture as the first step in developing the long-term program, recommended above, for dealing with the nuclear threat. This architecture and program should integrate, and create synergies among, all of the elements described below.

Information and Intelligence to Detect Nuclear Threat Operations. While it no longer requires the resources of a nation to build a nuclear explosive and transport it to a target, especially if the fissile material can be bought or stolen, neither is it a trivial undertaking. To build a nuclear device, a team must be assembled, funding obtained, security measures put in place, special facilities and capabilities provided for, and so forth. All along the time-line of such an operation, from initial planning to device emplacement, there are signatures which can be exploited by intelligence and/or law enforcement assets. Stealing or arranging to buy material or a weapon creates signatures, as does transportation to the target, including surveillance of the target and the access route. Most of these signatures may be small individually, but in aggregate they could be significant.

Experience has shown that even considerably less ambitious and less difficult terrorist operations take time and careful preparation, and therefore also have significant signatures. Although this is not always the case, it is often the case. Intelligence and law enforcement have often been able to exploit the signatures of such operations to deflect or defeat terrorist operations. The track record of the United States and our allies in recent years is considerably better than is commonly understood, perhaps mostly because it is the failures that make

¹⁰ A more in-depth treatment of the nuclear challenge, including over 30 detailed recommendations, appears in Annex C and in Volume III.

headlines. With their often greater signatures, there is the potential that nuclear threat operations could be detected for warning and interdiction.

While the potential exists to detect a nuclear threat operation, the current capabilities to do so are not sufficiently effective. The task force submits that there are ways to significantly improve the capability in all its dimensions. Probably the most important is to develop the capability to correlate many disparate, seemingly unrelated bits of information of many kinds, from all intelligence sources, and from many sources which may not be “intelligence” at all. Advanced information-management tools, including behavior and inference modeling, can help to pull significant information from large masses of data and guide analysts toward useful correlations. The interactive global information infrastructure, described earlier in this chapter, would be a key capability.

As part of an interactive global intelligence/information system, *the task force recommends that the Director, Central Intelligence and Secretaries of Defense and Energy integrate intelligence gathering and analytical tools for warning and interdiction of nuclear terrorist threats. This should be preceded by, and based on, development of an analytic capability to understand the interactions between nuclear threat operations and their signatures, and intelligence operations intended to detect them.*

Securing Nuclear Weapons and Materials. Experience in the United States and elsewhere shows that it is possible to achieve and maintain high levels of security for nuclear weapons and materials. Through the Cooperative Threat Reduction Programs in DoD and DOE, the DOE Nuclear Smuggling Program, and other efforts, the United States is working closely with Russia to improve weapon and material security, including providing hundreds of millions of dollars to supplement Russian funding in areas where US funding and competence provide high leverage on crucial needs.

It is clear to the task force that a *sine qua non* for further progress is continued US involvement and that, without some level of continued US funding, our influence will diminish. Most of the projects are programmed to wind down in the next few years. *The task force recommends that DoD and DOE commit to continue these programs for several more years, and seek authorization and funding from Congress.*

Over the longer term, fissile isotopes in the global civil nuclear energy fuel cycle are also a matter of concern, as they can be diverted for use in weapons. The International Atomic Energy Association and related safeguards are necessary but not sufficient for protecting these materials, which are stored in hundreds of places under a wide range of security measures. A more comprehensive, global regime is needed for protection, control, and accountability of these materials. The proposed Internationally Monitored Retrievable Storage System, which is one approach, is the subject of a current joint DoD/DOE study.

The Assistant to the Secretary of Defense for Nuclear and Chemical and Biological Defense Programs and the DOE Director of Nonproliferation and National Security should jointly develop a long-range plan to extend the Departments of Defense and Energy programs for securing nuclear materials and weapons in Russia, and to augment current international arrangements for securing weapon-usable material of all kinds, everywhere.

Threat Device Detection/Localization. Today, assets to detect and localize terrorist nuclear materials or explosives can be effectively deployed only at restricted choke points, such as ports of entry, or with intelligence warning that closely specifies threat location and time. To ease the requirements on intelligence, even as intelligence improves, it would be desirable to have continual coverage of much larger areas (cities or larger) as might be done with wide arrays of very large numbers of detectors or perhaps with fewer mobile detectors that could sweep large areas rapidly. But high false-alarm rates have made large arrays infeasible.

Recently, however, work has been done that indicates the potential for ameliorating this problem using a network logic that correlates "hits" among a large number of detectors using a model of scenario factors such as estimates or measured traffic flow rates between detector locations in a city. This filters out many false alarms. This, along with the potential for improvements in individual detectors of various kinds, for the first time opens a serious possibility of an effective wide-area detection and response capability.

The task force recommends that DoD and DOE jointly plan and assure funding for a program to develop and acquire capabilities to detect and localize the presence or transit of nuclear weapons/devices and materials over large areas, in conjunction with detection/search at ports and airports in the United States and overseas. This program should be directed at better force protection and protection in the United States. It should include a near-term advanced technology demonstration. The Department of Energy should lead in the addition of a long-term research and development program. This will require additional funds, some which should be devoted to high-risk ideas and/or ideas whose payoff may be further in the future.

The final phase of such a program should be to prepare to procure equipment in quantity and to train personnel so that, when needed, a capability could be quickly deployed to cover many large cities simultaneously. The National Guard should become an integral part of plans for such a large-scale surge capability. Planning and training for this should start now.

Disablement. A threat device that has been located could be booby-trapped to detonate when access or render-safe are attempted. Some nuclear devices, perhaps primitive ones especially, are not "one-point safe" – that is, attempts to destroy them could cause them to produce significant nuclear yield. There has been good progress in recent years in designing methods to preclude or limit such yield, but more should and can be done, and devices (such as advanced shaped charges) already known to be effective need to be procured.

The Department of Energy, the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict and the Assistant to the Secretary of Defense for Nuclear and Chemical and Biological Defense Programs should plan and assure funding for a single, coordinated program to develop and acquire greatly expanded capabilities to gain access to threat devices which have been located and to render them safe or destroy them with as little attendant damage as possible. The objective should be to have capabilities that closely approach the physics limits. This will require additional funds; some of these should be devoted to high-risk and/or future-payoff ideas.

Mitigation. While the consequences of a nuclear explosion would be cataclysmic, they can be partially mitigated. The program for ameliorating the consequences of terrorism involving the use of weapons of mass destruction is discussed at greater length in Chapter 2. Its most important feature is the institutionalization of the Nunn-Lugar-Domenici programs for first responders. *It is vital that nuclear consequences be included in this program as well. In addition, the Armed Forces Radiological Research Institute should complete the development of promising, improved treatment regimes for radiation-caused and radiation-exacerbated injury and promulgate its application among appropriate elements of the first-responder and medical communities.*

Attribution. Being able to correctly attribute a nuclear terrorism event to its perpetrators can help to deter the act itself and ensure that US responses are appropriate. It can also ameliorate the sense of helplessness that the public would otherwise feel after such an event. Improved detection capabilities, as discussed above, can also contribute to "after the fact" attribution, even if they fail to prevent an attack. In addition, there is a wide range of forensics technology that can complement other intelligence and detection capabilities before an event, and contribute to attribution after. One example is the analysis of minute samples of material, collected from the vicinity of suspected threat operations or from an explosion, from which information about the origin, history, and associations of the material can be obtained. Especially important is identifying worldwide reference data bases on nuclear materials and related data and establishing arrangements for rapid access to the data when needed.

Science and technology developed over the past several years offer rich potential for improving forensics capabilities, but are not being fully utilized. Nor are many resources being devoted to this area. *The task force recommends a several-fold increase for development of nuclear forensics technology.* This would represent only a small level of funding, compared with what is being spent to develop other capabilities, but one that could have significant return.

Radioactive Materials Dispersal. It is important to note that a nuclear explosion is not the only way to kill people or create a serious hazard with nuclear material. Radioactive material of many kinds can be dispersed easily over wide areas with standard chemical explosives or in other ways. Radioactive material used in medicine or industry exists in thousands of places and can easily be stolen. While such an event would not be as catastrophic as a nuclear explosion, it would be much easier to execute and thus harder to prevent. The measures and capabilities

discussed and recommended for dealing with the nuclear explosion threat will also expand the range of capability against dispersal events.

The Chemical and Biological Warfare Threat

Chemical and biological warfare agents share characteristics that make them an especially grave threat. They also have substantial differences that must be taken into account when devising strategies and postures to deal with them. The shared attributes include:

- They are relatively easy to obtain (certainly compared to nuclear) and potential users do not need access to large and expensive facilities to achieve potent capabilities.
- They can be developed and produced in laboratory or small scale industrial facilities which makes them difficult to detect. Also, the technologies required to produce them often have commercial applications as well, so their “dual-use” can be plausibly denied.
- They can be extremely lethal so small quantities can be very effective.
- They can be delivered by a variety of means.

While chemical and biological warfare agents are often grouped together (along with nuclear devices) as weapons of mass destruction, there are substantial differences in their effects. Perhaps the most important difference is that biological warfare agents can be far more toxic by several orders of magnitude than chemical warfare agents. Thus, the range of effects of a few kilograms of chemical agent could extend several city blocks. By contrast, the same amount of a biological agent could threaten an entire city.

A second significant difference is that, generally, the effects of chemical warfare agents occur much more rapidly – minutes to hours versus days for biological agents. The rapidity of effect was generally considered a positive attribute from the perspective of potential military use against troops on the battlefield. However, the delayed effects of biological warfare agents can work to the advantage of the transnational perpetrator, making covert delivery much easier and attribution much more difficult.

Chemical and biological agents can come in a variety of forms and lethal mechanisms (e.g., against food supplies as well as people) including the possibility of bioengineered new pathogens. However, “standard” agents like sarin (chemical) and anthrax (biological) pose a serious enough threat that one need not hypothesize new and novel agents. Thus, these deadly substances provide the means for individuals to threaten the many and allow the few to wage war, or long-term campaigns, against nations. A new breed of transnational actors, less interested in securing a seat at the table than in bringing down the house, may find considerable appeal in these weapons and their potential for mass casualties.

US concern about the chemical and biological warfare threat predates the current fear about the transnational threat. During the Cold War, the United States worried about the Soviet

Union's chemical and biological warfare programs, but our approach to dealing with this threat relied largely on our nuclear deterrent capabilities. The United States also complemented its nuclear deterrent posture with a modest capability to respond in kind to biological warfare threats, during the early part of the Cold War, and to chemical warfare threats for most of the Cold War. The United States eliminated its biowarfare offensive capabilities and programs in the 1970s and renounced any use of chemical weapons in the early 1990s. Within this deterrence-dominated strategic framework, direct defenses – either passive or active – against chemical warfare, and particularly biological warfare, rarely received high priority or sustained attention.

The Gulf War brought renewed concern about the vulnerability of US and allied military forces to chemical and biological warfare threats. While deterrence remained a vital element in the strategy against this threat from potential adversaries in regional conflicts, both passive and active defenses were appropriately deemed to play an increasingly important role. Subsequent to the Gulf War, DoD increased attention and resources to chemical and biological warfare defenses as part of its counterproliferation initiatives. Much of the passive defense effort, directed at protecting US military forces against the threat of chemical or biological weapons in regional contingencies, has relevance to the transnational chemical and biological warfare threat.

Combating The Threat. The biological warfare threat can appear so formidable and frightening that it can engender a posture of inaction. Indeed, it is too hard to find a perfect solution or a totally effective defense. There is considerable merit in former Navy Under Secretary Richard Danzig's prescription to "think small" with respect to defense against biological weapons. A focus on incremental steps that can help mitigate the threat and raise the price to potential attackers will more likely produce a sustainable and productive effort for the long term. Many new technologies offer the potential to build components of systems that will incrementally add to national capabilities to defend against this threat. This study, like others, while identifying many promising steps, found no silver bullet that will eliminate the entire range of threats.

Combating the transnational threat will require that our strategy and supporting posture be multi-element and provide "defense in depth." The elements of such a defense are well known and include dissuading and denying possession, deterring use, intercepting delivery, mitigating consequences, and identifying and punishing the perpetrators. However, the relative contributions and weights accorded to each element depend on the particular threat.

For the chemical and biological warfare threats, the elements needing most attention are consequence management and intelligence. The chemical and biological warfare threats require particular attention to consequence management. There are two reasons. While clearly it would be preferable to prevent incidents rather than mitigate them, the United States cannot count on prevention. The signatures for chemical and biological weapon production, storage, transportation, and delivery can be exceedingly small. By contrast, nuclear devices present much higher signatures and thus much greater opportunity for interruption earlier in the cycle. Thus we

must place very high priority on being prepared to deal with incidents involving chemical and biological agents.

The second reason is that defense and consequence management against chemical and biological weapon attacks can be very effective. Vaccines, detectors, masks, collective protection, and prompt medical treatment combined can make a huge difference in the outcome of an attack, perhaps reducing casualties by three orders of magnitude or more. This does not imply that there should be no effort on interdiction against chemical or biological weapons, but rather indicates where priorities should lie.

Intelligence and threat assessment activities are essential to addressing the chemical and biological transnational threats and to both prevent and respond effectively. In an ideal sequence one would look to intelligence support first for cueing, followed by confirmation, such that the threat is intercepted before any agent is disseminated. Should an event take place, then intelligence support would be critical for attribution. The approach for the chem/bio threat however, will require a significant departure from more traditional intelligence approaches, which are based on national technical means, because the signatures associated with acquiring a chemical or biological capability, especially by a transnational threat group, are low and ambiguous, and also are not completely understood. Cueing must therefore rely heavily on human intelligence, after which other intelligence resources – such as measurements and signatures intelligence or communications intelligence – can be targeted to help confirm acquisition and/or deployment activities. Should an event take place, the laboratory sample analysis capability of the threat assessment community will prove invaluable in identifying the perpetrators.

All of these efforts will be highly dependent on parallel information and data analysis capabilities that are drawn from any number of sources – open sources such as news sources; technical journals and conferences; transaction data bases such as purchases, shipments, or permit applications; law enforcement records; public health sources; and others. This is the basic rationale for proposing the Secure Transnational Threat Information Infrastructure.

In addressing this threat, significant investment must be made to develop analytical tools that target specific chemical and biological threats. Especially important for addressing the biological threat will be epidemiology studies that tie public health information on disease outbreaks with background environmental characterization to assess the unusual nature of the outbreak. Further, associating the outbreak of a disease with information on suspect production sites and/or with meteorological data could lead to pinpointing a facility for sampling and analysis. Effective intelligence of this sort will in turn depend on the availability of robust detection and field/lab analysis means to pull small signals from an extremely cluttered background.

Fully exploiting state-of-the-art knowledge engineering tools and information technology will be the critical enablers for the all-source assessment efforts that underpin every stage of intelligence support for this difficult threat. In addition, the need to disseminate the information

among many users and suppliers to the system will require sophisticated multi-level access/security architectures to allow entry to the system only at the appropriate "need-to-know" level.

DoD has unique capabilities among federal agencies to contribute to combating the transnational chemical and biological warfare threat. However, these capabilities are stretched thin and the underlying technology and resource base is fragile. DoD capabilities include long-standing units like the Army's Technical Escort Unit as well as recently generated assets such as the Marine Corps' Chemical Biological Incident Response Force. These units have missions that directly support domestic incident response, and as such, have tailored equipment and extensive training requirements. In addition Army Chemical units in both the active and reserve components have personnel trained in nuclear, biological, and chemical weapon protection, detection, and decontamination. Although their training and equipment is focused on the battlefield environment, it has application to transnational threat scenarios.

DoD's experience base for dealing with incidents involving weapons of mass destruction is growing through an increasing number of exercises and substantial involvement in preparing for both crisis and consequence management during high profile events like the Summer Olympic Games in Atlanta, the Democratic and Republican National Conventions, the 1997 Presidential Inaugural, and the Denver Summit of Eight Conference.

The Department has also made new investments in research and development activities to improve its capabilities to defend against chemical and biological warfare threats, such as 911-BIO, an accelerated growth of DARPA's biological warfare defense initiative, and coordination with DOE's Chem/Bio Nonproliferation Program.

Having recognized the Department's unique and impressive capabilities and commended DoD on its recent initiatives, the task force nonetheless is concerned about the downsizing pressures or "take-it-out-of-hide" edict to those organizations owning significant chemical or biological responsibilities. Of special note is the extremely fragile biological warfare defense expertise.

The task force endorses the Secretary of Defense's intent to add \$1 billion to the chemical and biological defense program as recommended in the Quadrennial Defense Review and recommends a number of steps to enhance the base of expertise capable of dealing with this threat.

- Enhance the Army Technical Escort Unit's ability to meet its expanding workload and support the local and federal law enforcement community (Federal Bureau of Investigation; US Secret Service; The Bureau of Alcohol, Tobacco, and Firearms; and state and local law enforcement) by enlarging the intelligence and communications sections and adding military personnel.

- Expand the teams which support the Combatant Commanders, as well as first responder training in biological and chemical warfare defense; the task force suggests a three-fold expansion as a minimum. To provide continuity, the government personnel assigned to this support should be civilian.
- Evaluate how expertise at the US Army Chemical and Biological Defense Command can be used to help develop force protection plans at US military bases. This command has the ability to leverage the Chemical Stockpile Emergency Preparedness Program, experience in working on emergency preparedness programs with local communities, as well as the equipment and technical expertise found at the chemical stockpile locations.
- Sponsor more interagency consequence management exercises and red teaming dealing with chemical and biological warfare that include all of the lead federal agencies – the Department of Defense, the Federal Bureau of Investigation, and the Federal Emergency Management Agency.
- Double the efforts of the Technical Support Working Group – the counterterrorism interagency development capability – on developing chemical and biological equipment to support military and appropriate civilian first responders.
- Leverage the extensive national expertise in biotechnology that is resident in universities and industry, as well as the research supported by federal agencies, which can greatly enhance DoD's capabilities in this area. Relevant expertise includes areas such as genetic screening, diagnostics, DNA sequencing, immunology, rapid drug developments, and point-of-care analytical capabilities.
- Establish a threat reduction program with the Russian biological warfare community. The extensive Russian biowarfare expertise and technology has the potential to migrate into the hands of transnational adversaries. Currently three small pilot projects are underway in an effort to mitigate such potential migration. *Much more needs to be done with the Russian biowarfare community and thus the task force recommends extending the Nunn-Lugar nuclear materials and weapons initiative to include similar efforts with biological warfare capabilities in Russia.*

The Information Warfare Threat

The transnational information warfare threat also poses significant technical challenges. Investigations into the security of DoD networks by the Armed Services and the Defense Information Systems Agency (DISA) have concluded that our networks are vulnerable to unauthorized access at the most intimate levels. The recently released Report of the Commission on Critical Infrastructure Protection reiterates the severity and importance of this threat to US national security. Tools and techniques for penetrating networks illicitly are rapidly becoming more sophisticated and varied, the associated software is easily available on the Internet, with instructions for its use, and there is a community eager to share and exploit these tools.

The intended effects of an information warfare attack probably will not be subtle. To surreptitiously compromise computer networks requires a long-term, dedicated effort of the sort most likely to be mounted by nation states or organized crime. Nation states whose motivation is intelligence gathering have the resources, patience, and finesse required. In the near term, transnational organizations could buy information from these sources but would not likely have an interactive capability. In the longer term, however, it is expected that motivated transnational adversaries will develop more sophisticated information warfare capabilities.

The impact on networks that a transnational group will likely be able to achieve will be disruptive (typically denial of service) and will be temporary in nature. Most DoD computer networks possess a redundancy and resiliency which reduces the likelihood of long-term interruption of service. Though the effect of a single attack is assessed to be temporary, a carefully orchestrated information warfare campaign can deliver sequential shocks to a system (or to multiple systems at once) extending the impact of the attack and creating cascading effects.

Because the potential impact of transnational information warfare attacks by themselves is considered to be temporary in nature, the central thrust of a significant attack will probably also entail high explosives or chemical, biological, or nuclear weapons. The information warfare dimension, if used, acts as an adjunct to impede emergency services and increase panic, and can also serve to amplify the psychological impact of other actions taken.

DoD's current network security posture is largely inadequate and the Department's unclassified networks have been compromised on a number of occasions. The known intrusions to date have been considered an annoyance or embarrassment rather than a threat, perceived as largely coming from amateur hackers. During the past five years, DISA has conducted a program known as the Vulnerability Analysis Assessment Program, which involves a series of planned information warfare intrusions on DoD organizations. In the five years of testing, DISA has attempted 49,540 intrusions, 70 percent of which were successful, with only 4 percent ever detected.

The Department has not yet begun to consider the impact of network disruptions from those with more malign intent, or to consider the impact of escalation from isolated incidents to a campaign of attacks with a directed purpose. Currently the US government has limited ability to detect the onset and execution of an information warfare campaign because there is no consistent reporting of incidents – malicious, accidental, or otherwise. Hence the fact that the intelligence and defense communities have not detected an information warfare “campaign” – as opposed to discrete probes – is cold comfort. We can only respond to the attacks we know about. Moreover, knowing that one is under a campaign-level attack requires, in addition to the data capturing events and the methods for categorizing them, analytical tools for distinguishing patterns in space and time among thousands of trillions of network events.

DoD needs to be able to recognize directed network attacks when they occur. The routine detection and recognition of network penetrations is not generally possible because there is no "culture of incident reporting" of anomalous incidents (and no clear definitions of what should be reported). There is no organized common repository for collection or analysis of incident reports within the DoD. Despite an increasingly critical reliance by the Department on commercial services, there is no process for receiving information on threat incidents from commercial organizations.

The task force urges DoD to address and solve the existing information warfare vulnerabilities that could interfere with its other functions and responses concerned with transnational threats. Moreover, widespread global information systems also present significant new opportunities that could assist the US Government in dealing effectively with these new problems. All DoD operations – both essential combat and important business applications – now rest on a foundation of critical information resources and processes. Joint Vision 2010, the current military strategy underlying US doctrine and operational concepts, demands "information dominance" as a core capability. However, this critical information infrastructure is no longer limited only to DoD-controlled networks and resources; DoD is increasingly reliant on the unclassified commercial national information infrastructure and the entire global information infrastructure for much of its crucial capability, including transmitting and distributing key classified data. The technology and knowledge exists in the public domain, and knowledge of these capabilities is widespread, to support a wide range of attacks of different types and degrees of impact on critical DoD and civil functions.

To forestall the bulk of low-level information warfare incidents, DoD should employ the concept of "Raising the Bar;" that is, raising standards of behavior and creating both technical and procedural barriers to easy intrusion into its networks. Doing this requires not just the imposition of technical measures and barriers but, more fundamentally, the creation of a culture that does not tolerate these activities even if they are merely annoying rather than severely damaging. It also implies that all potential attackers understand that they will be identified and dealt with aggressively; pranks and malicious behavior will be prosecuted so that a culture is created that understands the standards of conduct that need to be obeyed. Certainty of appropriate and calibrated retribution for all unsanctioned activities against information systems will communicate to all parties the costs of malign activities. Such a policy, if successfully implemented, and especially in concert with raising the bar against low-level incidents, would deter substantial numbers of potential problems.

To ensure adherence to proper procedures by users and operators, including the crucial incident reporting function, red teams should conduct unannounced penetration attempts on a frequent, but unscheduled basis using a wide range of techniques and capabilities. To ensure that malign activities are not risk or cost-free for the perpetrators, a policy of both aggressive "counter-attacks" and vigorous prosecution should be instituted. To facilitate these new initiatives, DoD should seek aggressive interpretations of legal and regulatory constraints on its information protection activities.

DoD must build the capability to improve its information protection abilities faster than the threats can create new methods for attack; this requires that processes for continuous improvement and organizational learning be an integral part of any DoD information assurance program. Information assurance standards or procedures that merely adopt best practices in existence at the time they are promulgated cannot maintain the needed degree of effectiveness in the dynamic environment presented by modern information systems and technologies. Learning from experience and incrementally improving practices, procedures, and systems is essential; continuous updating and refinement based on lessons learned from red team and forensic activities must be integrated into a dynamic set of information protection practices and become part of the operational and organizational culture.

Finally, DoD must understand that it is not alone; it exists within an increasingly seamless web of interconnected systems and users. Merely fixing its own internal systems by building perimeter defenses would not guarantee that DoD systems were secure from attack; multiple entry points to critical external functions and insider threats would still exist. Moreover, this narrow focus would provide no assurance that its critical suppliers, other government agencies, allied forces, or the national information infrastructure on which many of its activities depend would continue to function; these would remain vulnerable and also provide opportunities for denial-of-service attacks against critical DoD functions. DoD must, therefore, create structures that enable it to cooperate and share information with other government agencies, the private sector, and allied governments in addressing information assurance concerns.

Actions for Addressing “Too Hard” Problems

The task force recommends that DoD address the nuclear, chemical, biological and information warfare threats as part of broader architectural and planning efforts that respond to transnational threats. While recognizing that these are difficult challenges, the task force believes that the steps outlined in this report, and elaborated in more detail in the accompanying annex as well as in Volume III, can make a significant difference in the Department’s posture. The Secretary of Defense must take the lead in this effort, in cooperation with the Secretary of Energy, by directing the Department to define a set of initiatives to address solutions for mitigating the threats that have long been regarded as “too hard.”

Recommendation: Address the “Too Hard” problems in nuclear, chemical, and biological warfare defense and defensive information operations.

- ⇒ The Secretary of Defense and Secretary of Energy must task their respective departments to define and develop an expanded, cooperative set of initiatives to address solutions for mitigating threats and fulfilling needs that have been regarded as too hard.
- ⇒ The Joint Task Force, sponsored by the Joint Chiefs of Staff and the Under Secretary of Defense for Acquisition and Technology, must address in detail the “too hard” challenges.
- ⇒ The Under Secretary of Defense for Acquisition and Technology should implement science and technology and acquisition programs that focus on including long-term or high-risk solutions to problems often seen as too hard.
- ⇒ The President should raise the emphasis on this problem with an initiative to create significant awareness of the importance of addressing biological warfare challenges.
- ⇒ The costs of this effort:
 - ◇ For nuclear, cost in fiscal year 1999 is \$117 million
 - ◇ For chemical and biological warfare defense, cost in fiscal year 1999 is about \$300 million
 - ◇ For defensive information warfare, cost in fiscal year 1999 is \$200 million (cost details in 1996 DSB Defensive IW Report)

CHAPTER 4.

Summary of Recommendations

"To date this threat is becoming even more complex and difficult to counter as old and new bad actors take advantage of weak governments, new technologies, and rekindled ethnic rivalries."

SECRETARY OF DEFENSE, WILLIAM J. PERRY

CHAPTER 4. SUMMARY OF RECOMMENDATIONS

The task force has studied the issues surrounding transnational threats and made recommendations for a DoD response that includes six elements:

1. Treat transnational threats as a major DoD mission
2. Use the existing national security structure and processes
3. Define an end-to-end operational concept and system-of-systems structure
4. Provide an interactive global information system on transnational threats
5. Address needs that have long been viewed as “too hard”
6. Leverage worldwide force protection and civil protection

This task force asserts that an effective national response to the transnational threat and implementation of the six-element strategy requires a dedicated effort on the part of the President and senior leadership in the Department of Defense. To this end, the task force has identified a series of actions on which this senior leadership should focus.

The President should:

- ◆ Raise the emphasis on countering transnational threats in DoD, across the government, and with international coalition partner nations.
- ◆ Create an initiative to raise awareness of the importance of addressing nuclear, chemical, and in particular, biological warfare challenges.

The Secretary of Defense should:

- ◆ Treat countering transnational threats with the same emphasis as major military conflicts. As such:
 - Assign responsibility for transnational missions with greater clarity and assign, to a single policy office, responsibility for counterterrorism, counterproliferation, transnational threats and infrastructure protection.
 - Develop an architecture defining an end-to-end operational concept and a system-of-systems structure.
 - Elevate the priority of force protection plans and programs – in the departmental guidance and in the requirements and budget processes.
 - Direct the Under Secretary of Defense for Acquisition and Technology to develop the secure transnational threat interactive information system with the involvement of key federal, state, local, and international departments and agencies.

- Define and develop an expanded set of initiatives, in cooperation with the Secretary of Energy, to address solutions for mitigating nuclear, chemical, biological, and information warfare threats.
- Direct the Army to develop a plan to expand the scope of and institutionalize the Nunn-Lugar-Domenici program.
- Direct the Army and the National Guard Bureau to establish a national consequence management capability within the National Guard to support state and local agency responses to domestic chemical and biological incidents and to support the regional combatant commanders' Joint Task Force, when appropriate.

The Chairman should:

- ◆ Establish a Task Force within the Joint Staff to develop operational and systems concepts and architecture.
- ◆ Assign responsibilities for the military services to address requirements associated with transnational threats.
- ◆ Assign responsibilities for updating all operational plans for addressing transnational threats such that they include contingency planning, crisis response, and consequence management responsibilities.

The Under Secretary of Defense for Acquisition and Technology should:

- ◆ Establish a joint Technical Support Team that will provide analytical capabilities to support the Chairman in the development of a system-of-systems structure and architecture.
- ◆ Implement technology and acquisition programs which focus on mitigating "too-hard" problems.

In summary, the task force concludes that combating transnational threats is part of the Department of Defense's core business. The task force has determined that the Department can meet the challenges of this threat using existing policies and organizations. If the Department follows this course of action, the task force believes that the necessary resources will follow. Such an integrated, focused, and committed response will indeed allow the Department and the Nation to blunt the transnational threat.

ANNEX A:

Terms of Reference



THE UNDER SECRETARY OF DEFENSE
3010 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-3010



ACQUISITION AND
TECHNOLOGY

JAN 28 1997

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference - Defense Science Board 1997 Summer Study Task Force on DoD Responses to Transnational Threats.

You are requested to establish a Defense Science Board Study Task Force on DoD Responses to Transnational Threats. As the geopolitical structure of the Cold War collapsed, it enabled increased threats to the United States and its interests by organizations and individuals with motives and methods quite different than those posed to the nation during its confrontation with the Soviet Union. This trend has been recognized by the President in PDD-39 and by the Congress in various legislation covering threats to critical infrastructure, threats by transnational interests, and the proliferation of weapons of mass destruction. Each of these call for some form of implementation structure in the Executive Branch to provide for a government-wide, systematic response to some or all of this class of threats. This implementation structure has not yet evolved but the DoD will need to play its proper role. Of particular interest to the Chairman, Joint Chiefs of Staff is the protection of United States Armed Forces.

The nature of these threats are such that they are usually not located in or identified uniquely with any particular nation. In addition, their mode of operation often involves routine movement across national boundaries including those of the United States. The U.S. response requires therefore, the involvement of the federal, state and local law enforcement agencies, the national security community, and the national emergency response agencies. These circumstances call for an examination of the DoD posture with respect to these threats and its relationships with other Government elements that have critical roles to play.

The Task Force effort should provide an assessment of the DoD posture and recommend actions to improve this posture. Specifically, you are requested to:

- Review the legislation, executive orders, prior studies and current activities of the government,
- Identify the variety of threats which should be addressed by the Department,
- Assess the nation's vulnerability to these threats,
- Examine the DoD capabilities for playing its proper role in response,
- Identify available and potential technologies which may be applicable for enhancing the protection of US Armed Forces,
- Recommend actions by the Department to position itself properly for this set of problems.



The Task Force will be co-sponsored by the Chairman, Joint Chiefs of Staff and the Under Secretary of Defense for Acquisition and Technology. Dr. Robert J. Hermann will be the Task Force Chairman and General Larry D. Welch, (Ret) will be the Task Force Vice-Chairman. Ms. Regina Dugan, office of the Director, Defense Advanced Research Projects Agency will be the Task Force Executive Secretary. Maj. Wynne Waldron, will be the Defense Science Board Secretariat Representative. The Task Force will present a final briefing report 15 August 1997 and a final report within 60 days thereafter.

The Task Force will be operated in accordance with the provisions of P.L. 92-463, the "Federal Advisory Committee Act," and DoD Directive 5105.4, the "DoD Federal Advisory Committee Management Program." It is not anticipated that this Task Force will need to go into any "particular matters" within the meaning of Section 208 of Title 18, U.S. Code, nor will it cause any member to be placed in the position of acting as a procurement official.

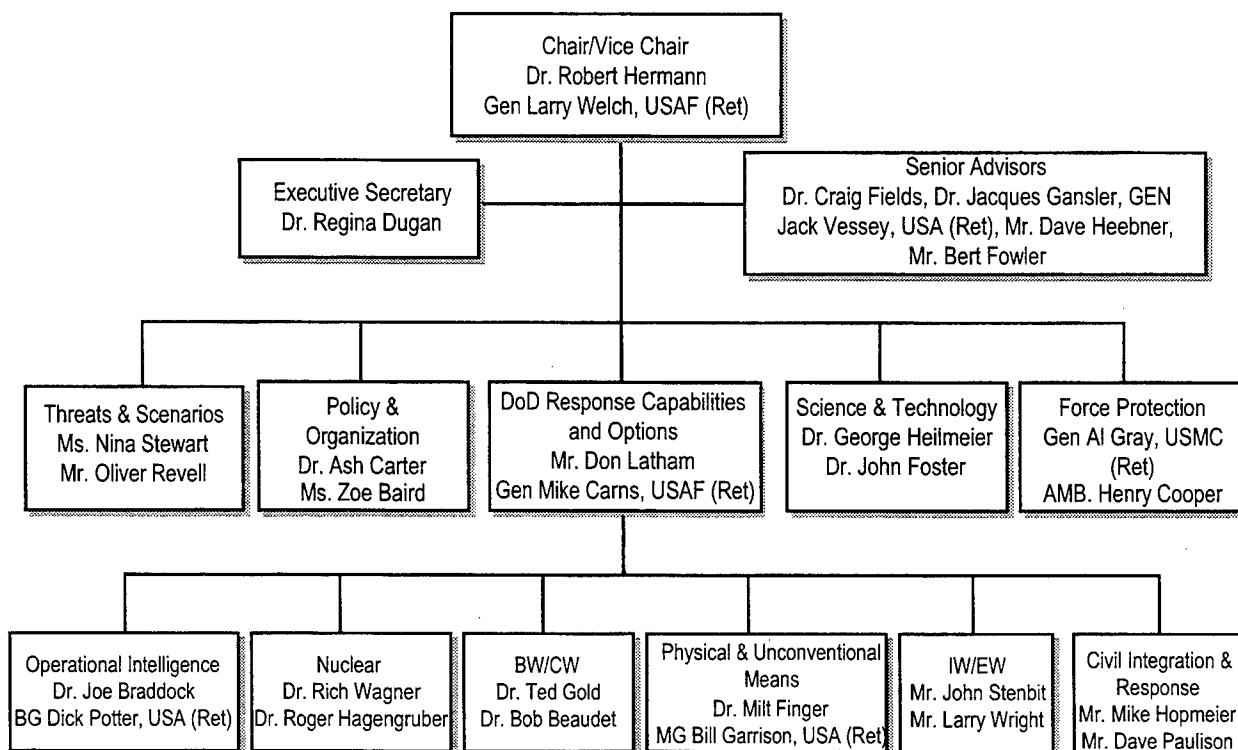
A handwritten signature in cursive script that reads "Paul Kaminski".

Paul G. Kaminski

ANNEX B:

Task Force Organization and Membership

Task Force Organization



Task Force Membership

Chair/Vice-Chair

Dr. Robert Hermann*
Gen Larry Welch, USAF (Ret)*

Executive Secretary

Dr. Regina Dugan

Defense Science Board Military Assistants

Maj Wynne Waldron, USAF, CDR Dave Norris, USN
LTC T Van Horn, USA

Senior Advisors

Dr. Craig Fields*, Mr. Bert Fowler*, Dr. Jacques Gansler*, Mr. David Heebner*,
GEN John Vessey, Jr. USA (Ret)*

Panel Membership

Threats & Scenarios

Ms. Nina Stewart
Mr. Oliver Revell
RADM Tom Brooks, USN (Ret)
Mr. Dennis Imbro
Mr. James Moody
Mr. Gordon Negus
Mr. John Capece
CAPT Jack Cassidy, USN
Dr. Larry Gershwin
Mr. James Hertsch
CAPT Keith Mulder, USN
Ms. Bonnie Phelps
Mr. Peter Probst
Maj Jon Ross, USMC
Mr. Jeff Staats

Policy & Organization

Dr. Ash Carter *
Ms. Zoe Baird
Mr. Frank Cilluffo
Hon. John M. Deutch
Dr. Richard Falkenrath
Mr. Steve Friedman
Mr. Richard Haass
Hon. Joseph Nye
Mr. Jeffrey Smith
Dr. Richard Weitz
RADM John T. Byrd, USN
Ms. Sheila Dryden
Mr. Larry O'Donnell
Mr. Douglas Perritt
Mr. Charles Swett

* DSB Member, ** Ex-Officio Member, *Government Advisor*

DoD Response Capabilities & Options

Mr. Donald Latham*

Gen Michael Carns, USAF (Ret)

COL John Fricas, USA

Operational Intelligence

Dr. Joseph Braddock
BG Richard Potter, USA (Ret)
Ms. Rebecca Beaty
LtGen Jim Clapper, USAF (Ret)
Dr. David Dye
Mr. David Geary
COL Kenneth Getty, Jr. USA (Ret)
Mr. Charles Hawkins
COL Thomas O'Connell, USA (Ret)
Dr. Dennis Polla
Maj Owen Devereux, USMC
Ms. Deborah Dewey
COL Don Faint, USA
CDR Bernie Hamm, USN
Mr. Wade Ishimoto
Mr. Paul Kozemchak
Ms. Beth Larson
CAPT Nelson Litsinger, USN
Mr. Theodore Royster
Mr. David Sanford
Col Stan Shinkle, USAF
Dr. Michael Shore
Col John Tempone, USMC
COL Butch Teston, USA
Mr. Thomas Warren
Mr. Kendrick Williams

Nuclear

Dr. Richard Wagner**
Dr. Roger Hagengruber
Mr. Gary Brown
Mr. Roland Herbst
Dr. Fred Ikle
Dr. George Miller
Mr. William Nelson
Mr. John Nuckolls
Ms. Amy Sands
Mr. Fred Wikner
Dr. Lawrence Woodruff
Dr. Mary Anne Yates
LTC John Betts, USA
Mr. Ronald Cosimi
Mr. Mark Monahan
Dr. John Immele
Col Dale Landis
Mr. Clifton McFarland
LtCol James Mueller, USAF
LtCol Michael Williams, USAF

BW/CW

Dr. Ted Gold*
Dr. Robert Beaudet
Dr. Robert Boyle
Dr. Jeffrey Grotte
Dr. Mim John
Mr. David Kay
Dr. Don Kerr
Dr. Donald Prosnitz
Dr. Brad Roberts
MG Jan Van Prooyen, USA (Ret)
Dr. Scott Ward
Dr. George Whitesides
LtCol Richard Benson, USAF
CAPT James Brick, USN
Dr. Lee Buchanan
BG Walter Busbee, (Ret)
MAJ John Drifmiller, USA
Mr. Raymond Geoffroy
LTC Al Hardy, USA
Dr. Anna Johnson-Winegar
Mr. Robert Joseph
CDR Mike McDermott, USN
Maj Ron Marks, USAF
Dr. M. Brad Parks
Dr. William Shuler
LTC Mike Urban, USA
Dr. James Valdes

Physical & Unconventional Means

Mr. Milt Finger
MG William Garrison, USA(Ret)
Mr. Jack Bachkosky
Mr. Paul W. Cooper
Dr. Terry Gudaitis
Mr. Jeff Harris
COL Paul Hutton III, USA (Ret)
Mr. Ira Kuhn
Dr. Al Brandenstein
Dr. R. Stephen Day
Mr. Robert Doheny
Mr. Donald Henry
Dr. Lyle Malotky
Dr. Randy Murch
Mr. Ed Phillips
Mr. Raymond Polcha
Mr. Chuck Sieber
Mr. Rick Strobel
Dr. Pat Vail
Mr. Kevin Wong

DoD Response Capabilities & Options (cont)

IW/EW:

Mr. John Stenbit *
Mr. Lawrence Wright
Mr. Duane Andrews
Mr. Jeffrey Cooper
Dr. Curtis Davis
Dr. Michael Frankel**
Mr. John Grimes
Mr. William Howard, Jr.*
Mr. Bruce M. Lawlor
Dr. Robert Mueller
Dr. Prasanna Mulgaonkar
Mr. Dennis Murray
Mr. Robert Nesbit
Mr. Mark Silverman
Mr. Robert Stein
VADM Jerry Tuttle, USN (Ret)*
Mr. Sam Varnado
Dr. Abe Wagner
Ms. Mary Dunham
Col(s) John Collier, USAF
COL Brian Fredericks, USA
Mr. Tom Handel
BrigGen Dave Nagy, USAF
Mr. Marion Oliver
LtCol Jim Rodgers, USAF
Mr. Howard Sequine

Science and Technology

Dr. George Heilmeyer*
Dr. John Foster*
Dr. Alan Berman
Dr. Greg Canavan
Dr. Robert S. Cooper*
Prof. Delores M. Etter*
Dr. Edward Gerry
Dr. Joshua Lederberg*
Mr. Peter Marino*
Mr. Walter Morrow*
Gen Randy Randolph, USAF (Ret)*
Dr. James Tegnolia
Mr. Vince Vitto
Dr. Alfred Brandstein
Mr. Roy Cooper
Dr. Joseph Dollar
Dr. Matthew Ganz
Dr. Helmut Hellwig
Mr. Richard Hess
Dr. Jasper Lupo
Mr. Paul Pillar
Mr. Earl Rubright
Mr. Tom Tesch
Mr. Frank Wattenburger

Civil Integration & Response:

Mr. Michael Hopmeier
Mr. Dave Paulison
Mr. Jeff Abraham
Mr. Cornelius Behan
Mr. Carlos Castillo
Mr. Phillip Chovan
Mr. Hank Christen
Mr. James P. Denney
Dr. Louis M. Guzzi, MD
Mr. Paul Maniscalco
Dr. Frederick Sidell
Dr. Annette Sobel, MD
Mr. John Timoney
MajGen Paul Carlton, USAF
CAPT Rob Carnes, USN
Mr. Bob Ruth

Force Protection

Gen Al Gray, USMC (Ret)*
AMB. Henry Cooper
COL Al DeProspero, USA (Ret)
LtCol Michael Janay, USMC(Ret)
Mr. John Kane
Mr. Robert Moore
Mr. Lou Moses
COL Dan Baur, USA
LtCol James Carothers, USMC
BGen Jim Conway, USMC
BG Billy Cooper, USA
Col Andy Corso, USAF
LtCol John Cowan, Jr., USMC
COL Dan Hahn, USA
COL Hal Johnson, USA
Mr. Roberto Mata
CAPT Arne Nelson, USN
COL Robert Neubert, USA
LtCol Roby, USAF
Mr. John J. Sloan
Mr. Dan Spohn

Support Staff

Ms. Barbara Bicksler
Mr. Christopher Bolcom
Dr. Nancy Chesser
Ms. Julie Evans
Mr. David Grienke
Mr. George McVeigh
Dr. Adrian Smith
Mr. Brad Smith, Jr
Mr. Iram Weinstein

ANNEX C:

Policy and Technology Recommendations for Enhancing DoD Capabilities

POLICY AND TECHNOLOGY RECOMMENDATIONS FOR ENHANCING DOD CAPABILITIES

This annex summarizes technology and policy recommendations for enhancing DoD capabilities and implementation approaches that expand on the general recommendations in Chapters 2 and 3. Further details can be found in Volumes II and III.

1. Interactive global information system on transnational threats¹

Information Processing. The task force believes that existing processes for managing intelligence information are out of balance. Currently the priorities for intelligence collection, the capability for multiple organizations to access needed clues and data in other organization's data bases, and the rule sets and techniques used by analysts to identify real or potential threats, needs to be refocused in order to more effectively address transnational threats.

Currently, the processing of relevant information is heavily dependent on name tracing. This process relies primarily on searching archived reports and data bases for prior mention of the names of individuals or groups that have appeared in a new report. Another commonly used technique is called link analysis. Analysts use link analysis to identify connections (telephone calls, face-to-face contacts, or other ties) that may indicate planning, preparation, recruitment, or support activities by an individual or group.

These and other techniques are employed to identify patterns in the operations of particular transnational groups. Analysts seek to determine the methods, area of operations, and preferred targets of a given group, relying mostly on information from past incidents. The ability to determine the relevance of information to a possible future event is limited.

The Task Force suggests that evolving techniques already employed widely in the commercial sector for searching, merging, sorting, and correlating data in multiple independent data bases can provide intelligence analysts with more effective tools than are now available to aid in discovering the identities, capabilities, intentions, and plans of foreign and domestic threat groups.

The Task Force recommends a new approach that fosters analyst teamwork, cooperation and collaboration; more automated support of the analysis process, and the development of technology for the search of heterogeneous distributed data bases. New techniques include:

- *Groupware for analysts.* Such a system would make use of modern object-oriented data base technology to handle multiple representations of data. It would also make the maximum possible use of modern data farming, mining, and warehousing techniques that

¹ The global information system is described in Chapter 3.

will facilitate development of search and recognition techniques, including those that employ context and content base search (latent semantic indexing).

- *Intelligent software agents.* Intelligent software agents can be focused to search for a confluence of events in multiple data bases or for goals over time. Profile filters can be used to identify recent activities and interests of threat organizations.
- *Tools to correlate all-source information* that will include both government and civil sector data bases.

Sensors. Currently, the primary source of data on transnational threat organizations and their operations involves the use of signal intelligence (SIGINT), open source information such as newspapers, embassy reports, and a very limited set of human agent reports (HUMINT). In addition, overhead imaging data provides some limited amount of information on terrorist training sites. Finally, limited data is also available from measurement and signatures intelligence (MASINT) collection assets that provide limited capabilities to detect various chemical, biological, and nuclear effluents at stand-off distances.

Because of the very high security consciousness of transnational groups, there is generally insufficient, verifiable information available about transnational adversary operations, membership, and other important details. Moreover, these groups often come from countries in which the United States has no human intelligence capabilities. As a result, little cueing information is available for placing short-range intelligence sensors capable of gathering signals intelligence, electro-optic, infrared, acoustic, and diagnostic data on transnational threat organization and weapons of mass destruction. In particular, current MASINT sensors have little capability to detect and identify biological warfare agent production, testing, and transport.

The task force suggests that the application of evolving technologies will permit the development and deployment of a new family of relatively covert sensors. If, on the basis of the improved information processing tools discussed in the preceding paragraphs, the locations of suspected transnational adversaries can be identified, these sensors can be used to refine our understanding of their plans and intentions. A review of evolving sensor and robotic technology has led the task force to believe that significant advancement can be achieved in the areas of:

- *Microrobots for the deployment of covert sensors.* A number of miniature sensors capable of obtaining electro-optic, infrared, acoustic, and trace effluent data either have been or are under development. The current means for deploying such sensors is severely limited because of the scarcity of human agents available for their deployment and because of the danger involved. Microrobots, both earth-traversing and airborne (in the form of micro unmanned aerial vehicles), have been proposed for covert deployment of micro-sensors. These sensors are covert in the sense that they are small and have a high probability of escaping notice. They can be camouflaged to appear as an insect, a small pebble, or a stick, for example. Techniques are under development to provide relatively covert communications back to a monitoring station. Among the techniques

being considered for this purpose are the use of optical fibers less than 10 microns in diameter.

- *Micro Tags (Sticky Electronics)*. With the advent of thin-film lithium polymer batteries and low-power electronic logic, it should be possible to develop micro-miniature active tags (of less than a few square millimeters in area) for marking material, vehicles, and equipment associated with suspected individuals or groups. As an example, these devices might have a GPS reception capability and would provide the instantaneous location of the platform onto which they have been caused to adhere. In order to conserve battery (and mission life) they would respond only when interrogated by a coded RF signal.
- *Bio-Marker Trace Detection*. When human beings work with certain materials or have been exposed extensively to a unique environment, their bodies develop specific antigens to these environmental effects. Consequently, if individuals have had extensive exposure to specific chemical, biological, high explosive, or nuclear materials and/or they have had extended stays in, and exposure to, the unique spores in specific target areas, their bodies will acquire specific antigens which usually are not present in the bodies of the general population. In effect the antigens constitute 'bio-markers' that, in coordination with other information, can be used to identify suspect individuals. The best means of identifying these antigens would of course be via blood samples. If, as is likely, it is infeasible to obtain a blood sample from a person not in custody or charged with a crime, then other means will be required to obtain a sample for antigen analysis. As future technology is improved, antigens might then be detected at national entry portals as trace contamination on emigration documents or passports, by urine analysis, or by other means. With improved detection sensitivities as exemplified by the DARPA program to develop an artificial "dog's nose," it should be possible to identify some potential transnational adversaries by the antigens they carry.

Additional Intelligence-Related Recommendations. The task force makes a variety of recommendations for enhancing the operational intelligence capabilities of the DoD:

1. The Secretary of Defense should unify the operational focus on transnational threats.
 - Assign combating transnational threats mission to the combatant CINCs.
 - Task the combatant CINCs to assess current operational intelligence capabilities and recommend improvements.
 - Task the combatant CINCs to formulate plans to unify transnational threat operational intelligence.

2. The Secretary of Defense should improve intelligence analysis capabilities.
 - Task the National Security Agency, Central Intelligence Agency, and Defense Intelligence Agency to jointly reengineer the analyst paradigm and demonstrate the capability in the Counter Terrorism Center, within the next two years.
 - Task each military service to provide the status of implementation of the recent DoD directive to expand the Foreign Area Officer program (DoDD, 1315.7).
 - Task the Director, Defense Intelligence Agency, to formulate a resource requirements plan for expanding defense intelligence analytical capabilities to provide necessary coverage of transnational threats.
3. The Secretary of Defense should take steps to improve clandestine operations.
 - Request the President's Foreign Intelligence Advisory Board undertake a review of laws, policies, and regulations which limit collection and slow approval of planned actions and recommend changes that could be made (by the Executive Branch; propose to Congress).
 - Task the Director, Defense Intelligence Agency, to take the lead in developing and publishing a comprehensive reference on transnational threats to guide operational commanders.
4. The Assistant Secretary of Defense for Intelligence should task intelligence agencies to provide immediate use of appropriate operational intelligence to first responders.
 - Task the Director, Defense Intelligence Agency, to formulate procedures similar to those used in the past (examples: NATO, Korea, Bosnia, Gulf War) to address dissemination of DoD classified information to selected first responders.
 - Introduce DoD solution into interagency environment to establish an acceptable and workable community solution.

2. Force Protection

Selected force protection recommendations are summarized below. A more complete treatment of force protection recommendations is contained in *Volume II – Force Protection*. The Task Force believes that DoD should strengthen the technology initiatives supporting force protection, as discussed in Chapter 2. The following areas of emphasis are suggested:

- *Enhanced perimeter security* - rapidly deployable sensor systems, closed circuit TV monitor, vehicle explosives detection, tags/tracking, deployable barriers.
- *Extending the perimeter* - thermal imager for wide area surveillance, covert ground-based sensors, unmanned aerial vehicle sensors, microrobotics, special signals intelligence techniques.

- *Rapid, continuous inspection of vehicles* - measuring mass, x-ray, and neutron sensors for large vehicle screening, trace detection, "smart" nose, chemistry on a chip, and canine olfaction.
- *Protection enroute* - common missile warning systems, Global Positioning System monitoring to detect jamming and spoofing.
- *Intelligence, indications and warning* - force protection fusion terminal, biological and chemical warfare sensors.
- *Neutralization of the threat* - biological and chemical warfare countermeasures, high power microwaves, ultra violet sterilization of biological warfare agents.
- *Reducing the consequences* - construction and glass hardening, shock attenuators.
- *Enhanced exercises and training* - PC assessment methodology, red force exercises, real time gaming.

Force Protection Test Bed. As a mechanism for transitioning promising technologies into field use, this task force also recommends that DoD develop a force protection test bed (or test beds) and conduct a five-year plan for rapid technology insertion, including demonstrations in the following areas:

- Covert sensors to extend the perimeter, remote vehicle weigher, thermal imaging to extend the perimeter, advanced entry control.
- Automated sentry (3-D multispectral assessment/detection).
- Integration of covert ground-based sensors into force protection.
- Deployable force protection package (modular/robust, high/low technology, support elements).
- Force protection associate (all-Service intelligence, global information, real-time language translation, source validation).
- Biological and chemical weapon sensor networks.
- Construction hardening.
- Emerging technology using unmanned aerial vehicle/aerostats (change detection - SAIP, multispectral 3-D imager, ground-based sensors).
- Active defense against missiles and indirect fire.

Additional Recommendations for Force Protection. The task force also made a number of other specific recommendations regarding science and technology initiatives supporting force protection and the broader mission of countering transnational threats:

- Task the military services and DARPA to develop and implement a force protection "associate" to support local commanders.

- Assign the military services responsibility to:
 - Acquire application-relevant clutter data for laser-based standoff chemical and biological weapon detection systems.
 - Monitor and exploit industry “lab on a chip” initiatives.
 - Partner with Federal Aviation Administration on high-explosive detection systems.
- Assign DARPA responsibility to:
 - Develop and test bio-markers as indicators of personal activity.
 - Develop and demonstrate a gamma ray camera.
 - Evaluate field effectiveness of ultra violet radiation to deactivate micro organisms and virus in aerosols.
 - Develop and demonstrate microrobot sensor deployment systems.
 - Develop “sticky paper electronics” concepts.

3. Dealing Effectively with the Nuclear Challenge

This section elaborates on the task force recommendations, introduced in Chapter 3, to deal effectively with the nuclear challenge.

Detecting Threat Operations. All along the time-line of building a nuclear device, from initial planning to device emplacement, there are signatures which can be exploited by intelligence and/or law enforcement assets. The task force makes the following additional recommendations specifically for nuclear aspects of the transnational threat.

- The Secretaries of Defense and Energy should ensure that, as other task force recommendations for intelligence are implemented, the nuclear dimension is explicitly addressed.
- The Department of Energy, with the assistance of the intelligence and law enforcement communities, should support development of an end-to-end architecture. Also, to aid operational planning, a tighter linkage of counter-terrorism users of intelligence nuclear analysts and intelligence collectors should be established to understand the interactions between nuclear threat operations and their signatures, and intelligence operations intended to detect them. This increased understanding should be reflected explicitly in an analytic framework or model.
- The Department of Energy, with the intelligence and law enforcement communities, should re-establish a sound and enduring science and technology intelligence analysis capability in the nuclear area. This will involve recruiting, training, and equipping a cadre of analysts with the necessary technical backgrounds and exploiting the resources of the national laboratories more effectively. It should also include a plan for a surge

capability in the analytical cadre since incidents of terrorism tend to be somewhat episodic.

Securing Nuclear Weapons and Materials. The present DOE Material Protection, Control and Accounting (MPC&A) and DoD Cooperative Threat Reduction programs to secure the nuclear weapons and material within Russia should be extended beyond 2002. The United States should encourage Russia even more strongly to consolidate its nuclear and weapons materials in fewer sites, and should provide ongoing financial, technical, and moral support for projects beyond MPC&A, such as warhead dismantlement, plutonium disposition, and plant closings. The Russian MPC&A system should be coordinated with local response elements.

The task force also recommends:

- The Department of Energy, DoD, Customs, and FBI should cooperate in the development of a safeguards culture in Russia's Ministry of Atomic Energy and Ministry of Defense that should be extended to export and border control agencies.
 - Attention should be focused on helping the Russians deal with the insider threat.
 - Continue the lab-to-lab programs and US support for the projects of the International Science and Technology Center.
- Share studies and technology for polygraphy and methods for effective red-teaming.
- The Department of Energy should develop a comprehensive, international, long-term program to secure weapon-usable nuclear materials. The program should be extended to other states possessing special nuclear materials, in part via the International Atomic Energy Agency's new International Physical Protection Advisory Service or by other bilateral means.
- The Department of Energy and the State Department should urge the nuclear supplier states of the west to buy all highly enriched uranium available outside of Russia in the newly independent states, thereby eliminating the urgency of developing a safeguards culture and system in at least six countries.
- Convert research reactors from highly enriched uranium to low-enriched uranium fuel.
- The Department of Energy should monitor the security of reactor fuel of certain reactor types (breeder and naval) within the former Soviet Union.
- The Department of Energy should sponsor a long-term MPC&A System for the global civil fuel cycle that builds on the current International Atomic Energy Agency and national efforts.
 - Support the proposed Internationally Monitored Retrievable Storage System (IMRSS) currently under joint study by OSD and the Department of Energy.

- The Department of Energy's nascent R&D program on proliferation-resistant fuel cycle technologies should be expanded to include collaborative R&D with other nations including Russia and China.
- The Department of Energy should develop new technology and systems for automated, continuous monitoring of high-risk materials and nuclear processing.
 - Examine the "tagging" of sensitive nuclear materials so their movement can be monitored and, if ever lost, be tracked and identified quickly upon recovery.

Detecting the Presence or Transit of Nuclear Material or Weapons. DOE and DoD should plan and fund a program to develop and acquire capabilities to detect the presence or transit of nuclear weapons/devices and materials over more ambitious areas and should continue efforts to respond with shorter warning time.

This and the next two recommendations suggest a strategy for acquiring an integrated system of radiation detectors and response forces to screen as well as search much larger areas: as a basic building block the task force urges the Department of Energy to develop and deploy at least a few dozen next-generation Modular Application Search Systems (MASS), adaptable for vehicle or fixed application, and incorporating next-generation data processing and networking capability as well as advanced detectors.

DoD and DOE should work toward the development of a system of several hundred (maybe even a thousand) networked sensor modules for nuclear search and screening in urban environments, to screen harbors or ports, and for base protection. These should be portable and might be derived from MASS, but would exploit computing and communications among the detectors to reduce false positives. In the long term, the network and MASS would be based on advanced detectors and methods developed in the program recommended below.

DOE should establish a continuing test program to characterize time-dependent radiation patterns in urban environments and to test and demonstrate networks as well as individual sensors in the proposed architecture.

DOE should expand current efforts to develop next-generation sensors applicable not only to "terminal defense" of limited areas but broadly applicable to detection and interdiction of stolen nuclear material. The task force believes that this will require additional funds and that some of these resources should be devoted to high-risk ideas. For example, smart detectors show promise to eliminate false and nuisance positives with an emphasis on room-temperature operation, reduced size and unit costs, and automated spectral analysis. Gamma-ray imaging is also very promising. In the far term this may hold the revolutionary promise of distinguishing small radiation signals against background radiation over large areas (square kilometers of area every few seconds). In the near term, less ambitious angular and spectral resolution will permit application to smaller search areas (5,000-50,000 sq. meters) and to device diagnostics. Finally,

sensor concepts (probably active) exist for detecting highly enriched uranium and shielded material.

Gaining Access to Threat Devices, and Rendering Them Safe with as Little Damage as Possible. Progress can be made on this set of problems only with more resources and that is what the task force recommends. On the basis of studies and R&D already done, we believe that with affordable levels of further R&D and procurement, it is feasible to develop access and render-safe capability which will be effective for a wide range of (though not all) scenarios in which such capability is relevant. Developing this capability can serve to narrow the range of winning options for the potential adversary.

This task force recommends that DoD and DOE:

- Develop diagnostics which describe more accurately and from more remote distances the mechanical assembly and electrical/booby trap construction in an improvised or stolen nuclear device.
- Add additional resources and personnel to perform technical and operational device assessment to determine if a device is capable of producing nuclear yield and, if so, how various render-safe options would affect the yield. The task force is encouraged that this work will help attract and train the next generation of stockpile stewards. (*DOE only*)
- Focus development on new methods of rendering safe the remaining classes of nuclear devices not covered by existing methods. Several improved techniques could be used to negate weapons that are not accessible, safe to defuse, or of known design. One is the use of very high velocity, explosively driven projectiles. Such projectiles are well developed, and their extension to higher velocities is not stressing. If successful, these projectiles should produce little or no nuclear yield; however, they are sensitive to uncertainties about the design of the device. An alternative disablement mechanism, which has been studied less intensively, is a thermal blanket or microwave source. The Departments should ruggedize the new methods for military use in the field, and test under as near real conditions as is possible. These new systems should be deployed in sufficient numbers (i.e., more than one) to respond quickly.

Consequence Management. The program for ameliorating the consequences of weapons of mass destruction are discussed at greater length elsewhere in the report. An important feature is institutionalizing the Nunn-Lugar-Domenici programs for first responders. Nuclear consequences should be included in this program as well. For example:

- DOE, FEMA, and DoD need better planning and preparedness, not just for a radiological or weapons accident but for the sheer devastation of an actual nuclear detonation.

- DoD should continue, under Nunn-Lugar-Domenici, to establish the nation-wide training program for first responders, including nuclear consequence management.
- Train the National Guard for nuclear, chemical, and biological consequence management and exercise a nationwide linkage of DoD and the National Guard with first responders. Use the National Guard for training & equipping.
- The Armed Forces Radiobiology Research Institute should complete the development of improved treatment regimes for radiation-caused and radiation-exacerbated injury and promulgate its application among appropriate elements of the first-responder and medical communities.

4. Responding to the Chemical and Biological Warfare Threat

The current systems and capabilities have many deficiencies.²

Nerve Agents. Nerve agents are difficult to detect and characterize at standoff distances. The counteragents used – atropine, pyridostygmine hydrobromide – are themselves toxic, and require care in use. Protective gear is expensive, since nerve agents are toxic by skin contact: there is no effective protection for rear echelon personnel, or for large numbers of civilians. Decontamination following an attack is difficult and slow and involves caustic and reactive solutions (e.g., bleach), and there are no established criteria for declaring an area safe once it is decontaminated.

Other Chemical Agents. Many of the same criteria apply to blister, nerve, and blood, and to other agents that have been considered and developed by some nations.

Biological Toxins. Biological toxins – especially botulism toxin, staph enterotoxin, ricin, and abrin – are more toxic than nerve agents and have the additional feature that symptoms may not develop for more than 12 hours after exposure. It is therefore difficult to detect an attack by the response of the population that has been exposed. Treatment of these agents is possible if they are detected early, but the detection methods are slow and expensive. For some, once symptoms have developed, treatment is limited to support. There are no methods of detecting these agents at standoff; detection at short range generally requires immunochemical methods, and is relatively slow (15 minutes after sample collection) and expensive. There are no accepted methods for sampling air and soil to detect these agents. Biological toxins, in general, require that they be breathed or ingested to be toxic, and relatively simple masks afford useful protection; these masks are not available in the quantities needed to protect rear echelon military personnel, ports, airbases, and civilian populations. Decontamination is again slow and labor intensive, and there are no simple methods for declaring an area safe.

Pathogens. Pathogens such as anthrax, tularemia, plague, glanders, cholera, and Q fever pose the most difficult problems in detection and characterization. There is no standoff detection and only limited point detection. The tests that are available now require access to what is effectively

² The chemical and biological warfare threat is discussed in Chapter 3.

a biology laboratory. Since symptoms do not develop for several days after exposure, it is possible, in principle, to have an attack expose large numbers of people, particularly in a terrorist attack on a civilian population, with no indication that an attack had taken place. Since some of these diseases are highly contagious, there is a serious problem of managing a biological attack in such a way that it does not lead to epidemic. In a biological attack, there is a crucial problem of separating those who have been exposed and require treatment from those who have not been exposed; there is no technology for triage now. Protection of the caregivers in the system – from first responders to hospital personnel – relies on conventional methods such as protective clothing and isolation, and the system would be overwhelmed in any serious attack. Decontamination will vary with the agent. There is no accepted set of protocols for decontamination and for certifying that affected areas are safe, especially for anthrax, which is persistent in spore form.

There are a number of new technologies that are applicable to various parts of the biological and chemical warfare defense problem. This area is one in which there is no “silver bullet” that will nullify the entire range of threats. Rather, these technologies offer the potential to build the components of systems that will add substantially to national capabilities in defense.

- *Characterization.* Molecular biology is offering a broad range of tools for genetic classification of organisms that will provide one of the keys to identification of the entities used in an attack. These tools, based on methods for genetic sequencing and for identification of proteins, enormously expand capabilities in this area. They are, however, still slow and expensive, they require skilled personnel to use them, and they must be made more rugged. The excellent work going on in this area should be aggressively pursued including work in biochemistry on a chip, genetic sequencing of threat organisms, microfluidic systems, rapid genetic identification, application of mass spectroscopy to biological assays, and a range of others. A key issue for the DoD is the development of systems that are effective in field use.
- *Collection.* Unmanned air and ground vehicles offer new opportunities for collection and standoff detection. One of the characteristics of biological and chemical weapons is that they are usually airborne, and large-area dissemination would require spreading them in the open air. This type of attack could be blunted with early warning by unmanned aerial vehicles equipped either as detectors/collectors (with characterization being done elsewhere) or with on-board microanalytical systems. Sensors developed for such use would also be applicable as point sensors.
- *Stand-off Detection: New spectroscopic methods.* A range of techniques – differential infrared absorbency or reflectance, ultra-violet fluorescence, hyperspectral analysis – offer opportunities for some stand-off detection. Airborne mass spectroscopy or other microanalytical methodology may offer additional capabilities.
- *Area Defense through Area Sterilization by Ultra Violet.* It is possible that some area protection can be achieved by using local ultra violet pathogen neutralization. “Ultra

violet searchlights” might be used to irradiate the pathogen cloud and deactivate at least part of it. This type of technology would not provide complete protection, but it would decrease the area that was contaminated.

- *Improved Protocols for Vaccination.* Vaccination is an effective method of decreasing the threat of disease. The most dramatic decreases in morbidity and mortality from infectious disease in civilian populations have come from successful vaccination, not from the much more expensive and problematic treatment of disease. For many possible components of a biological attack, there is no treatment once symptoms appear: pulmonary anthrax, botulism and ricin toxicity, and essentially all viral diseases fall in this category. Prevention is much more effective than response in biological and chemical warfare. Applied immunology has been an area of enormous advance in science; very little of the advance in this area has been applied to the problem of biological warfare defense.
- *Early Detection of Exposure/Disease.* A range of techniques can be used to examine populations for early signs of disease, well before the development of overt symptoms. Early rises in levels of key chemical signals for inflammation and activation of the immune system are among them. The development of field tests that can distinguish the population of those individuals who had been exposed from those who had not would be an enormous contribution to the management of biological incidents. There is less of a problem with chemical incidents, since the development of symptomology is more immediate and more obvious.
- *Aids for Intelligence: Biomarkers.* A system for examining the exposure of animals and people to past environmental influences is now possible in principle, and would provide new tools for analysts (although it would also require new methods of operations).

5. Information Warfare

In recent years, the problems associated with protecting the Defense Information Infrastructure against attack have received much attention.³ The concern of designers of DoD information systems has been to defeat intrusive attacks which may result in the destruction and exploitation of vital data files and to defeat attacks that may result in the denial of information services. Denial of service attacks include any attacks that will limit the DoD's ability to transfer information electronically. Such attacks may include the jamming of communication links – both military and civil – and attacks which saturate the ability of terminals to receive and process incoming data. Other forms of attack may include message alteration or the insertion of false messages by someone who is successfully masquerading as (or actually is) a valid user of a DoD network. Such attacks may result in the degradation of the integrity of some DoD data bases and files, with the associated possibility of inappropriate actions being taken.

Information technology is being developed at an extremely rapid pace in response to the ever-expanding commercial demands. As a result, the technology necessary to defend the system must also be developed on a continuous basis. There is no single new approach. A number of

³ Chapter 3 contains an introduction to the information warfare threat.

broadly based programs are currently being pursued by both DoD and commercial industry. These approaches, which should provide a significant increase in the robustness of the Defense Information Infrastructure, include:

- *Improved barriers* that respond automatically to the threat of attack such as policy driven access control; software modules or 'wrappers' for the protection of legacy and commercial off-the-shelf components; and more robust protection of the communication infrastructure.
- *Enhanced intrusion detection and response* systems that improve coordination of detection and response functions and software to provide better cooperation between intrusion detectors and boundary controllers.
- *New adaptivity and resource management* techniques.
- Employment of *artificial diversity*.

The task force makes the following specific recommendations in the area of information warfare:

- The end-to-end operational concept, recommended in Chapter 2, should include the integrated offense/defense architecture and the system-of-systems solution elements for information warfare described in this annex. The foundation of the recommendations is an architecture approach that uses a feedback mechanism for dynamic improvement; therefore, all elements of the architecture must be implemented to accomplish the full benefits.
- Information warfare readiness should be included in the Joint Staff process. Definition of readiness should be based upon a set of standards and metrics developed by a DoD assigned defensive information warfare information center (411). Information warfare readiness, per se, should be tested, measured, evaluated, and reported as part of the normal JCS readiness reporting system (as described in the DSB report, *Information Warfare-Defense*, November 1996).
- For information warfare architecture elements, the following reorganization of existing assignments and responsibilities should occur. An information warfare 911 operations center for the reporting of all information security related incidents should be assigned to the Joint Staff. While the Defense Information Systems Agency currently has part of this assignment and might be the basis for expansion, the task force does not believe they are capable of doing this even with major augmentation. Forensics should be assigned to the Information Operations Technology Center located at Fort Meade. Specialized talents needed to perform forensics will be scarce and must be gathered from wherever they reside, including defensive information warfare, Air Force/OSI, other National security agencies, and the Computer Incident Response Teams. The 411 center should be assigned to the Information Operations Technology Center. This requires IOTC to embrace and

implement defense information warfare as a priority. Red Team leadership should be assigned to J3. Populate team from national Security Agency, the Joint Command and Control Warfare Center, etc. These organizational elements can be created within current funding levels via reassignment and reprioritization of responsibilities.

- The Under Secretary of Defense for Acquisition & Technology should include, in all contracts and requests for proposals, a requirement for suppliers to report all attacks on information systems to the 911 center. Suppliers should also be required, in proposals, to describe their capabilities to detect attacks on information systems, and to describe what reports the 911 center should expect. The effectiveness of supplier capabilities to detect and report information warfare incidents can be used as an evaluation discriminator. Suppliers should be permitted, and encouraged, to use the 911 center.
- The ASD C3I should direct that DoD and supporting information systems move away from a perimeter defense concept for defensive information warfare towards a "distributed partitioned secure enclave concept."
- DoD should enhance interface with state and local first responders. Task DISA to assemble, equip, train, test, and maintain an order wire. Allow first responder to establish communications. This will require procurement of Public Safety Standard Radios (APLO-25), use of MILSTAR, and should include deployable Local Area Network/Wide Area Network.

6. Civil Integration and Response

This report addresses the need for civil integration in Chapter 2, including the participation of civil first responders from key cities in the United States. The following recommendations are made in this area:

Information Management

- Implement a standing panel to act as representatives of the first response community (i.e., firefighter, paramedic, law enforcement, emergency medicine) to the Federal Strategic Planning Community.
- Establish a single point of contact for access to information and support from the Federal Government for the first response community (training, intelligence, technology, response, etc.). Too much confusion and misinformation exists for the current system to be effective.

Training

- Training needs to be focused on institutionalizing efforts within the civilian community, not forcing it from the outside. The proper role of DoD is in creating basic information and techniques with the first responder community providing its own training.
- Institute a program for providing experts and advisors to local communities as and when needed for the formulation of plans and programs and for advice on training and exercises.

- Provide a method of standardization and evaluation on effectiveness of local community efforts that applies consistent standards and provides for changes as conditions and information warrant. Also, include a validation method for information to ensure accuracy and validity, not rumors and hearsay.
- Accept the Incident Command System as doctrine for federal assistance to first responders and provide training to relevant military personnel in the Incident Command System.
- Provide standardized, realistic training information and goals for first responders.

Strategic Concerns

- Resolve conflict between various federal agencies and within DoD on issues of support, training, and response. Where practical, obtain certification and approval for use of military equipment in civilian environments.
- Implement a technology transfer program, allowing for both development and deployment of military technologies and equipment.
- Use the Tri-Care system or Congressional legislation to encourage adopting extended training regimes and exercises for use by the first responder community in combating unconventional threats.
- Provide straightforward, consolidated, and rational methods to fund first responder training, preparedness, and response.

Intelligence

- Take greater advantage of potential human intelligence resources in the first responder community.
- Create a data base of domestic incident sites, with evaluations, analyses, and lessons learned, that can be accessed and used by the first responder community.
- Implement a system to disseminate critical information and provide for first responder access to classified data – The Secure Transnational Threat Information Infrastructure as described in Chapter 3.
- Create and implement a coordinated and consistent response policy (similar in concept to the Federal Response Plan) that applies to both federal and civilian assets.

ANNEX D:

Summary of Laws and Executive Branch Guidance Documents

SUMMARY OF LAWS AND EXECUTIVE BRANCH GUIDANCE DOCUMENTS

This appendix summarizes relevant laws, executives orders, departmental directives, and federal response plans that guide Department of Defense (DoD) programs and activities in support of civilian agency responses to transnational threats.

Posse Comitatus. Posse Comitatus was enacted after the 1876 presidential elections. This act precludes the use of federal troops in the execution of civilian laws. No one has ever been prosecuted under this act, due in part to the ambiguity of the language making Court interpretations difficult. In 1981, Congress attempted to clarify the role of the Defense Department by enacting U.S.C. 10 Sections 371-378. Each section defines how, when, and to what extent military personnel can be used to respond to civilian emergencies:

- In Section 371, the Secretary of Defense (SECDEF) must provide information collection during the normal course of military operations that complies with the Privacy Act and can be provided to civil law enforcement.
- Section 372 authorizes the SECDEF to provide equipment, base facilities, and research facilities to federal, state, or civilian law enforcement officials for law enforcement purposes. This includes disposing of old military equipment as well as loaning sophisticated equipment. This section does not include the use of non-government facilities under contract with DoD.
- Section 373 expands the role of DoD by authorizing the Secretary of Defense to provide training to civilian law enforcement on the operation and maintenance of equipment provided in Section 372.
- The last two sections expand on the different cases in which military personnel could be used in civil scenarios and the regulations that should be in place to protect civil liberties. The Secretary of Defense is authorized to use military personnel in a limited capacity in narcotics cases. The SECDEF is also authorized to use military personnel upon written request from a Federal agency head stating that a mission will not be successful without the aid of military personnel. This could involve passive use of the military for maintaining and operating equipment. The SECDEF should enforce regulations which prohibit direct military participation in search, seizure, arrest, or similar activity, unless authorized by law. The SECDEF should also ensure that any of the above-described use of military personnel does not adversely affect the military preparedness of the United States.

In emergency situations, several exceptions are incorporated into Posse Comitatus. Authorization for military assistance must come from the President in the form of an Executive Order. The request for military assistance from civilian authorities must be made through the Attorney General. The military can be called to assist civilian law enforcement should the civilian law enforcement authorities be unable to enforce the law, or are impaired without assistance, or there is a serious threat to US interests.

Emergency Preparedness. *The Robert T. Stafford Disaster Relief and Emergency Assistance Act (PL 93-288)* chartered the President as the lead authority for disaster preparedness. As such, the President is responsible for establishing the means for granting disaster relief and declaring a state of emergency. Once a declaration has been made, emergency support teams can be formed. The act also establishes a system for reimbursing agencies and assistance programs involved in disaster relief. Most of this authority is now delegated to the Director of the Federal Emergency Management Agency (FEMA) under Executive Order 12148.

Executive Order 12656: Assignment of Emergency Preparedness Responsibilities authorizes the President to establish national security emergency policy through the National Security Council. FEMA assists in the implementation of the policy. Each agency/department is required to develop a system for response that addresses protecting essential resources, defining succession in the office, ensuring continuity of essential office functions, and conducting training. Each agency or department is the lead for certain responsibilities during an emergency.

Military Directives. *Department of Defense Directive 3025.1* consolidates the Department's policy for military support to civil authorities applicable to disaster-related civil emergencies within the United States and with those related to attacks on the United States, previously known as "Military Support to Civil Defense." It states the policy and responsibilities of the Department in responding to major disasters or emergencies in accordance with the Stafford Act, as amended, and supports the national civil defense policy and federal or state civil defense programs, in cooperation with FEMA, under the authority of the Federal Civil Defense Act of 1950. The scope of this directive includes all planning and response by DoD for civil defense or other assistance to civil authorities but does not include military support to civil law enforcement operations, that is addressed in DoD Directive 3025.12.

Department of Defense Directive 3025.12 updates the Department's policy on planning and responding to requests for military assistance to federal, state, and local governments in the event of civil disturbance and operations, which includes responding to terrorist incidents. This directive appoints the Secretary of the Army as the DoD Executive Agent for military assistance for civil disturbances. The use of military forces for civil disturbances can only be authorized by the President through an executive order which directs the Secretary of Defense to respond to a specified jurisdiction under specific circumstances. In certain cases, it may be necessary to use military forces before obtaining Presidential authority. In these situations, the DoD officials or commanders will use all available means to obtain Presidential authorization while applying their emergency authority. The Attorney General will manage the federal response to civil

disturbances. The request for military support shall come from the Attorney General in response to an official request by a state or federal civil law enforcement or Executive authorities. This directive does not include responsibility for response to aircraft piracy or counterdrug operations. These are addressed by other agencies or under other legal authorities. The remainder of the directive addresses specific responsibilities given to different DoD components.

Department of Defense Directive 3025.15 establishes DoD policy and assigns responsibilities for providing military assistance to civil authorities. Under this directive, the Department's policy is to cooperate with and provide military assistance to civil authorities as directed by and consistent with applicable law, Presidential Directives, and Executive Orders. This directive defines the criteria necessary in order for military assistance to be used in civilian emergencies, such as, DoD support to civil disturbances or DoD responses to acts of terrorism. The request for active duty military forces to aid in domestic civil disturbances may only be made by the President or Attorney General and authorized only by the President. The use of US military forces for domestic counterterrorism operations may only be made and authorized by the President (or in accordance with Presidential Decision Directives). All requests for assistance in responding to acts or threats of domestic terrorism must also be approved by the Secretary of Defense. This directive details the authorization procedure for a request of military support; for example, requests for emergency support during natural or man-made disasters should be made through the Secretary of the Army. DoD's posture in response to acts or threats of terrorism are to be managed by the Secretary of Defense. The remainder of the directive defines responsibilities specifically assigned to offices within the Department to keep officials updated on situations in which military assistance is exercised.

Department of Defense Directive 2000.12 delineates the DoD Combating Terrorism Program. Specifically, this directive updates the Department's policies and responsibilities for implementing the DoD Combating Terrorism Program pursuant to the "Public Report of the Vice President's Task Force on Combating Terrorism," February 1986; assigns responsibilities for the protection of Department personnel and their families, facilities, and other material resources from terrorist acts; continues to authorize the publication of "Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence" as the DoD standard for force protection against acts of terrorism, in accordance with DoD Directives Systems Procedures; establishes the Chairman of the Joint Chiefs of Staff as the principal advisor and focal point responsible to the Secretary of Defense for all DoD force protection issues; and expands the responsibilities of the Combatant Commanders to ensure the force protection of all DoD activities in their geographic area of responsibility.

Under this directive DoD is to protect personnel and their families, facilities, and other material resources from terrorists acts in accordance with the published handbook "Protection of DoD Personnel and Activities against Acts of Terrorism and Political Turbulence." When applying this standard, commanders and managers are required to assess the mission, the threat, and specific circumstances which may require higher levels of force protection or which may justify deviations from the standard. The directive establishes guidelines for anti-terrorism

protection and training, for physical security of all DoD activities both overseas and in the continental United States, and for elevating the awareness of terrorist threats to DoD personnel and their families in high threat areas. This directive also assigns anti-terrorism responsibilities to specific offices within the Department.

Department of Defense Directive 3020.36 assigns specific responsibilities to DoD Components for National Security Emergency Preparedness. This directive updates policies and assigns responsibilities for developing emergency preparedness measures to enhance DoD's readiness posture. These measures focus on cases of implementation with little or no time constraints and on ensuring continuity of government during any national security or domestic emergency situation. Plans should focus on the aptitude of each DoD component to survive, recover, and reconstitute their functions during an emergency. This directive assigns specific responsibilities to several DoD components during an emergency. For example, the Director of Defense Research and Engineering is to supervise or conduct research related to emergency preparedness, advise other DoD components in planning for research in their specific area, represent the Department on interagency task forces on research related to emergency preparedness, and provide guidance for augmenting the Department's scientific and technical capabilities in a crisis. These emergency plans and actions will not be implemented unless the authority is provided by a law from Congress, an order is issued from the President, or a directive or order is issued by the Secretary of Defense.

Other Laws and Regulations Related to DoD's Response Options:

1. Under *Sections 12301 et seq of Title 10 United States Code*, the Secretary of Defense may order Reserve Components members to active duty without consent not more than 15 days a year. The Secretary may retain, with consent, the members on active duty anytime. During a national emergency, the Secretary may also order members to active duty. The Secretary may not order members or reserve units to active duty for a disaster, accident, or catastrophe.
2. The *Insurrection Act (Section 331-35 of Title 10 United States code)* can be employed if a Presidential proclamation to insurgents is made and an executive order is given to the Attorney General and the Secretary of Defense. Once the requirements have been satisfied, this code allows the Secretary of Defense the necessary use of federal troops to quell civil disturbances, enforce federal laws, and guarantee civil rights or enforce court orders.
3. The *Economy Act (Section 1535, Title 31 United States Code)* authorizes federal agencies to provide supplies and services to each other. It also mandates that there be cost-reimbursement associated with the supplies and services rendered.
4. *Executive Order 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions*, establishes the National Telecommunications System

(NCS). This system consists of assets from 23 departments and agencies which comprise the NCS Committee of Principals. One of the missions of the NCS is to assist the President, the National Security Council, the Director of the Office of Science and Technology Policy, and the Director of the Office of Management and Budget in coordinating the planning for and provision of national security and emergency preparedness communications for the Federal Government under all circumstances, including crisis or emergency, attack, recovery, and reconstitution.

The Secretary of Defense is designated as the Executive Agent for the NCS. As Executive Agent, the Secretary of Defense is responsible for designating the Manager of the NCS; ensuring that the NCS conducts unified planning and operations, in order to coordinate the development and maintenance of an effective and responsive capability for meeting the domestic and international national security and emergency preparedness telecommunications needs for the Federal Government; ensuring that the activities of the NCS are conducted in conjunction with the emergency management activities of FEMA; recommending, in consultation with other principals, the assignment of implementation or other responsibilities to NCS member entities and recommending new initiatives to assist in the exercise of the functions specified earlier; and overseeing the activities of and providing personnel and administrative support to the manager of the NCS, and providing staff support and technical assistance to the National Security Telecommunications Advisory Committee, established by Executive Order No. 12382.

5. *Nunn-Lugar I* addresses the prevention and control of proliferation of weapons of mass destruction (WMD). The proliferation of weapons of mass destruction has become a major security threat for the United States in the last decade. This law focuses US policy on both limiting the supply and demand of weapons for mass destruction as well as preparing the US to respond to an attack should one occur. The legislation suggests that priority should be given to technology and acquisition programs. To avoid duplication of effort and achieve maximum efficiency in use of resources, the law establishes a Joint Review Committee. Congress felt that initial attempts by the defense and intelligence communities to consolidate and coordinate proliferation programs would not provide a permanent solution. Thus, the Joint Review Committee could educate policymakers in understanding the strengths and weaknesses of US counterproliferation policies and influence budget decisions in an attempt to maximize the output from investments across departments and agencies. The Committee requested that the Secretary of Defense submit to Congress a report which contained data on existing systems and programs related to counterproliferation, a detailed review and evaluation of the resources allocated, and an inventory of programs and activities at the national and service laboratories. The report should also address specific steps to correct inefficiencies.

6. *Defense Against Weapons of Mass Destruction Act of 1996*, commonly referred to as Nunn-Lugar-Domenici, establishes DoD as the lead agency in the Emergency Response Assistance Program. Congress found that the United States lacked adequate measures to counter an attack involving the use of weapons of mass destruction. State and local responders are not adequately prepared or trained for a WMD incident and exercises involving the coordination and preparedness of federal and local responders have revealed major deficiencies. Therefore, it became essential to establish a program where a lead agency would use its expertise and resources to provide civilian personnel of federal, state, and local agencies with training and expert advice on emergency response to the use of weapons of mass destruction.

Under this act, the Secretary of Defense is to coordinate with FEMA, DOE, and other agencies with expertise in responding to emergencies and to provide training in the operation and maintenance of equipment for detecting chemical or biological agents, monitoring agents, protecting emergency personnel and the public, and decontamination. The SECDEF is also to establish a "Hot Line." On October 1, 1999, the President may appoint a new lead agency for this program. The SECDEF is also required to develop and execute a plan to test the preparedness of the federal, state and local responders to emergency situations which may involve biological and/or chemical agents. This plan should be executed each year beginning with fiscal year 1997, and should include other agencies such as FEMA, DOE and the FBI as appropriate. The first of these exercises was held in Denver in the Spring 1997. A similar plan is to be developed by the Secretary of Energy for situations involving nuclear weapons.